Ursinus College

Digital Commons @ Ursinus College

Number Theory

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

Summer 2023

Lagrange's Study 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 Study of Wilson's Theorem

Carl Lienert*

June 30, 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 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. As Lagrange explained:[4]

> I have just found, in an excellent work of Mr. Waring that I recently received, a beautiful arithmetic[5] theorem, ...
>
> . . . . . .
>
> 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."

*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.

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

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] While Lagrange gave fair credit to Waring and Wilson, he also seems to have been proud of his proof. In fact, Lagrange not only gave the first published proof of what today is known as Wilson's Theorem in this paper, but demonstrated its mathematical connection with work of Pierre de Fermat (1601–1665), stated and proved the converse of Wilson's claim, and even provided a second proof of Wilson's Theorem. In this project, we will work through each of Lagrange's proofs to gain a better understanding of the "beautiful arithmetic theorem" proposed by Wilson.

1 Theorem Statement[7]

Lagrange began with a statement of the theorem, known today as Wilson's Theorem, that he had found in Waring's work:

> *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.

Let's start with some of the computations that Wilson must have performed:

Task 1 Verify Wilson's Theorem for $n = 2$, $n = 5$, and $n = 7$.

It would be interesting to know how many values of n Wilson checked. For $n = 17$, the number to check has 14 digits.[8] Lagrange recorded the result through $n = 13$ in his paper, finding for that value that $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 + 1 = 13 \cdot 36846277$.

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

[7] Our section organization in the rest of this project follows that of Lagrange's paper.

[8] Optional Task: Verify that 17 divides $16!+1$, but without using a calculator or other modern computational device. One way to do this is to start with Lagrange's result for $12!+1$ as a short cut to calculating $16!+1$, then divide by 17. Although this project intentionally avoids modular arithmetic notation since Lagrange would not have used it either, another way to do this would be to use modular arithmetic to show that $16! \equiv -1 \pmod{17}$. If you are familiar with modular arithmetic, try doing it both ways to experience the power of "good" modular notation.

When initially thinking about the problem statement it's also natural to wonder if the statement is, in fact, true for *any* positive integer n.

Task 2 If you remove the condition that n be prime, is the theorem true? Justify your answer.

Task 3 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?

2 A Lemma

Today, a proof of Wilson's Theorem is typically given using a result known as Fermat's Little Theorem.[9] Lagrange presented a different proof, and he explained why, as we'll see.

Lagrange started his proof with a computation that he labeled a lemma. His organization was, perhaps, more natural than the way that mathematical results are often presented today. Modern textbooks often present the statement of a theorem or lemma as a finished result *before* the computation that provided the insight. We'll follow Lagrange's organization: we'll start with the computation and look at the statement of the lemma later. The initial set up of Lagrange's computation was:

Given the continual product:

$$(x+1)(x+2)(x+3)(x+4)\cdots(x+n-1),$$

we propose to expand it according to the powers of x.

We see that we'll have

$$\begin{aligned}&(x+1)(x+2)(x+3)(x+4)\cdots(x+n-1)\\&\quad= x^{n-1}+A'x^{n-2}+A''x^{n-3}+A'''x^{n-4}+\cdots+A^{(n-1)}\end{aligned}\tag{1}$$

and in order to easily determine the coefficients $A', A'', A''', \ldots$ we note that the preceding equation above is an identity [and] will equally remain [true] in putting there $x+1$ for x; which is why we will also have:

$$\begin{aligned}&(x+2)(x+3)(x+4)(x+5)\cdots(x+n)\\&\quad=(x+1)^{n-1}+A'(x+1)^{n-2}+A''(x+1)^{n-3}+A'''(x+1)^{n-4}+\cdots+A^{(n-1)}\end{aligned}\tag{2}$$

Pay careful attention to what Lagrange did! In (1), Lagrange wrote the form of the expansion of the product according to powers of x. In (2), it's tempting to think he similarly expanded the product on the left side of the equality. That's not what happened though.

Task 4 What did Lagrange do? How is the right side of (2) similar to that of (1)?

[9] We'll see Fermat's Little Theorem and its connection to Wilson's Theorem later in this project.

Lagrange continued:

. . . multiplying (2) by $x+1$, and then comparing it to (1) multiplied by $x+n$ we'll have . . .

Task 5 If you do what Lagrange suggested in this excerpt to the left sides of (1) and (2), how do the left sides of the equations that you obtain *compare*?

Task 6 Perform the same operations to the right sides of (1) and (2) and write down the identity that results. You don't need to "simplify" (yet).

According to Lagrange, you should have:

$$(x+n)\left(x^{n-1}+A'x^{n-2}+A''x^{n-3}+A'''x^{n-4}+\cdots+A^{(n-1)}\right)$$
$$=(x+1)^n+A'(x+1)^{n-1}+A''(x+1)^{n-2}+A'''(x+1)^{n-3}+\cdots+A^{(n-1)}(x+1), \quad (3)$$

that is, expanding the terms and ordering them with respect to [powers of] x,

$$\begin{aligned} x^n &+ (n+A')x^{n-1}+(nA'+A'')x^{n-2}+(nA''+A''')x^{n-3}+\ldots \\ &= x^n+(n+A')x^{n-1}+\left[\frac{n(n-1)}{2}+(n-1)A'+A''\right]x^{n-2} \\ &\quad+\left[\frac{n(n-1)(n-2)}{2\cdot 3}+\frac{(n-1)(n-2)}{2}A'+(n-2)A''+A'''\right]x^{n-3}+\ldots \qquad (4)\end{aligned}$$

Task 7 It is relatively easy to see how to obtain the left side of (4). Give a brief explanation.

It takes a little more work to be convinced that the right side of (4) is correct, and to see where the rational expressions in n come from. To expand the right side of (3) we need a simple case of the Binomial Theorem:[10]

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

Task 8 Expand the right side of (3) for $n=5$, and collect like terms according to powers of x. Resist the temptation to simplify the fractions that appear as coefficients. For example, leave $\frac{5\cdot 4}{2}$ as it is instead of simplifying to 10.

[10]We write the Binomial Theorem in the format Lagrange would have known it. Modern binomial coefficient notation was introduced by the Austrian mathematician Andreas von Ettingshausen (1796–1898) in 1826. See https://mathshistory.st-andrews.ac.uk/Miller/mathsym/stat/.

Task 9 For a general n, what would the next term in (4) be?

Task 10 For $n = 5$, use (4) to compute the values for A', A'', A''', A'''' by comparing coefficients of the powers of x.

Task 11 Check your result for Task 10 by expanding $(x+1)(x+2)(x+3)(x+4)$.

Lagrange provided the result you found in Task 10 in general. This general result is the lemma that he set out to prove in this section of his paper, which he stated as follows:

Thus, since this equation (4) is an identity, comparing term by term, we'll have:

$$\begin{aligned} n + A' &= n + A', \\ nA' + A'' &= \frac{n(n-1)}{2} + (n-1)A' + A'', \\ nA'' + A''' &= \frac{n(n-1)(n-2)}{2\cdot 3} + \frac{(n-1)(n-2)}{2}A' + (n-2)A'' + A''', \ldots \end{aligned}$$

from which we obtain:

$$\begin{aligned} A' &= \frac{n(n-1)}{2}, \\ 2A'' &= \frac{n(n-1)(n-2)}{2\cdot 3} + \frac{(n-1)(n-2)}{2}A', \\ 3A''' &= \frac{n(n-1)(n-2)(n-3)}{2\cdot 3\cdot 4} + \frac{(n-1)(n-2)(n-3)}{2\cdot 3}A' + \frac{(n-2)(n-3)}{2}A'', \end{aligned} \tag{5}$$

and so forth.

Task 12 What is the next line in the "and so forth"?

And more importantly:

Task 13 What is the last line in the "and so forth"? *Hint*: For what value of n would your answer to Task 12 be the *last* line, and for that value of n how does that line simplify?

It's worth pausing for a moment to appreciate what Lagrange did to obtain the lemma stated in this last excerpt. He considered a simple product $(x+1)(x+2)\cdots(x+n-1)$ from two perspectives: at x and at $x+1$. By comparing the view from these two perspectives he was able to develop a system of equations that allowed the iterative computation of the coefficients of the expansion. The form of these iterative expressions for $A', A'', \ldots$ were what allowed Lagrange to make his final conclusions, as we'll see.

A second strategy Lagrange employed was to move the question into a "larger" arena. The statement of Wilson's Theorem is about positive integers. Lagrange attacked the problem not in the ring of integers but in the ring of polynomials.[11]

[11] Lagrange would not have thought about the settings as *rings* since that concept was not yet developed. He would have used the term *Theory of Equations* for *ring of polynomials*.

3 A Corollary to the Lemma

At this point in his paper, Lagrange had developed formulas for the coefficients of the powers of x in the expansion of

$$(x+1)(x+2)(x+3)\cdots(x+n-1).$$

Remember, n is a prime number.

He next used these formulas to obtain a useful corollary.

> It is clear, by the theory of equations, that the coefficients $A', A'', A''', \ldots$ are nothing other than sums of natural numbers $1, 2, 3, \ldots n-1$ inclusively, products of these numbers in pairs, triples, etc.; in such a way that the last coefficient $A^{(n-1)}$ will equal the product $1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1)$; thus all the numbers $A', A'', A''', \ldots$ will necessarily be integers.

In the first part of this statement Lagrange essentially asserted that a product of polynomials with integer coefficients has integer coefficients; in other words, all of the coefficients $A', A'', \ldots$ are integers.

In the second part of this statement Lagrange made a specific observation about the constant coefficient, $A^{(n-1)}$, which turned out to be particularly important.

Task 14 Explain why $A^{(n-1)} = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1)$. *Hint*: Go back to equation (1) in the setup of the lemma in Section 2.

4 The Main Theorem

Next, Lagrange (re-)stated his main theorem and provided a proof:

> With the same notation as in the preceding lemma, I say that, if n is a prime number, the numbers $A', A'', A''', \ldots, A^{(n-2)}$ inclusively are all divisible by n, and that the last number $A^{(n-1)}$ is divisible by n, having been augmented by one.

Task 15 Which part of this statement is Wilson's Theorem?

We'll now follow Lagrange's proof step by step.

We know the expressions

$$\frac{n(n-1)}{2}, \frac{n(n-1)(n-2)}{2\cdot 3}, \ldots, \frac{(n-1)(n-2)}{2}, \frac{(n-1)(n-2)(n-3)}{2\cdot 3}, \ldots$$

always denote whole numbers, as long as n is a whole number; since they are the coefficients of a binomial raised to the power n, or $n-1$, or etc.

Lagrange explained that these expressions are the coefficients obtained when expanding an expression like $(a+b)^n$.

Task 16 Confirm that the coefficients of the expansion of $(a+b)^4$ are of the form given in the except above.

Task 17 Explain why the coefficients of $(a+b)^n$ (or, equivalently, $(a+b)^{n-1}$) must always be whole numbers.

Lagrange continued:

Further, it is clear that, if n is a prime number, the numbers

$$\frac{n(n-1)}{1\cdot 2}, \frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}, \ldots \tag{6}$$

will all be divisible by n, with the only exception of the last number

$$\frac{n(n-1)(n-2)\cdots 1}{1\cdot 2\cdot 3\cdots n} \tag{7}$$

which is equal to one; because it is seen that the numerator of each of these numbers is divisible by n, and that the denominator is not, as long as n is prime; from which it follows that after having divided the numerator by the denominator, the factor of n will remain in the quotient.

Task 18 Why is it true that the denominators of (6) are not divisible by n? Hint: Remember that n is prime here.

Task 19 The "last number" (7) appears in your answer to Task 13. Which term in your answer is it?

Finally, Lagrange finished the proof of Wilson's Theorem in two steps:

From there and from the formulas in the preceding lemma it is easy to conclude: first: That A' will be divisible by n, that $2A''$ will also, and the same of $3A'''$, $4A^{\mathrm{IV}}, \ldots$ until $(n-2)A^{(n-2)}$; and that as a consequence the numbers $A', A'', A''', \ldots, A^{(n-2)}$ that we have seen must always be integers, will be themselves divisible by n, at least when n is prime.

Task 20 Explain why each of $A', 2A'', 3A''', \ldots, (n-2)A^{(n-2)}$ is divisible by n. Lagrange gave a hint: start with A', etc.

Task 21 Why does this imply that, in fact, each of $A', A'', A''', \ldots, A^{(n-2)}$ is divisible by n?

Task 22 The last part is up to you: Use Task 13 to solve for $A^{(n-1)} + 1$ and complete the argument "that the last number $A^{(n-1)}$ is divisible by n having been augmented by one."

And thus Lagrange proved the statement of Wilson as reported by Waring!

5 A Second Corollary

The story didn't end with Lagrange's proof of Wilson's Theorem however. Lagrange also noticed a connection between his proof and "the famous Theorem of Fermat for which Euler has given several proofs." The famous theorem that he had in mind here is today often called Fermat's Little Theorem and states the following:

Fermat's Little Theorem.
If p is prime, and a is relatively prime to p, then p divides $a^{p-1} - 1$.

In short, Lagrange showed that Fermat's Little Theorem follows from his proof of Wilson's Theorem as a corollary. We'll again follow his proof step by step to see how he did this.

Lagrange started his proof of this corollary with:

In general, it follows from the formula (1) that for any integer x

$$(x+1)(x+2)(x+3)\cdots(x+n-1) - x^{n-1} + 1 \tag{8}$$

will always be divisible by n as long as n is a prime number.

Task 23 Explain how (1) and the results about the coefficients $A', A'', \ldots, A^{(n-1)}$ show this statement.

Lagrange then considered two cases: when x is divisible by n, and when it is not. First:

If x^{n-1} is divisible by n, which can only happen when x is zero or a multiple of n, the number

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

will always be divisible by n, which gives the Theorem of Mr. Wilson by making $x=0$.

Here, Lagrange stated, a second time, the result of Wilson's Theorem.

Task 24 Lagrange didn't explain. How does this follow from (8)?

The second, perhaps more interesting, case is when x is not divisible by n:

If x is neither zero nor divisible by n, which happens when $x=\mu n+\rho$, where ρ is any integer less than n, it is clear that one of the numbers

$$x+1, x+2, x+3, \ldots, x+n-1$$

will necessarily be divisible by n, and the product

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

will as a consequence always be divisible by n; thus $-x^{n-1}+1$, or rather $x^{n-1}-1$ will in this case always be divisible by n; which is the famous theorem of Fermat for which Mr. Euler has given several proofs in the *Commentarii Academiae Scientiarum Petropolitanae*. Ours, as one sees, has the advantage of showing the connection and the mutual dependence of the two Theorems.

Task 25 Why did Lagrange think his proof was better than those of Euler?

Let's follow the steps in Lagrange's proof:

Task 26 Lagrange was a little careless when he wrote "...where ρ is any integer less than n ..." Give an inequality for the integer values of ρ that Lagrange intended.

Task 27 What theorem allowed Lagrange to claim "$x=\mu n+\rho$, where ρ is any integer less than n?"

Task 28 Why must one of the numbers

$$x+1, x+2, x+3, \ldots, x+n-1$$

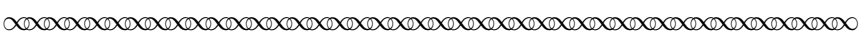
be divisible by n?

Task 29 Make the final argument explicit: how does the statement that n divides $x^{n-1}-1$ follow from the divisibility statement about (8)?

Thus, Lagrange showed that both Wilson's Theorem and Fermat's Little Theorem follow, by cases, from one and the same divisibility statement.

6 First Remark: Converse to Wilson's Theorem

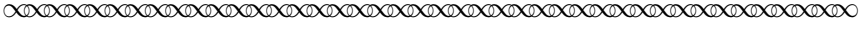
Lagrange next proved the converse to Wilson's Theorem, in the first of three "remarks" at the end of his paper. We start by re-stating Wilson's Theorem:



If n is any prime number, the number

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots (n-1) + 1$$

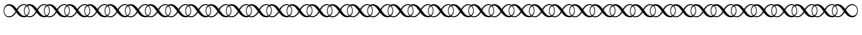
will always be divisible by n;



Task 30 State the converse of Wilson's Theorem.

Task 31 Demonstrate the converse with at least two numerical examples.

Lagrange's proof of the converse was concise:



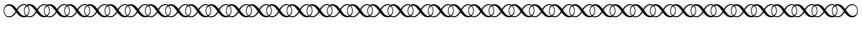
... if n is not prime, the number $[1 \cdot 2 \cdot 3 \cdots (n-1)+1]$ that we have seen must be divisible by n under the hypothesis that n is prime, will no longer be. Because if n is not a prime number, it will thus be divisible by one of the numbers $2, 3, \ldots, n-1$ less than n. Thus if

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

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 32 Explain why the first sentence of this excerpt is equivalent to the converse of Wilson's Theorem. Your answer to Task 30 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 33 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 34 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 33 in mind.

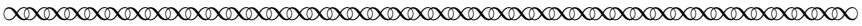
Task 35 Rephrase the statement

> "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 36 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 35?

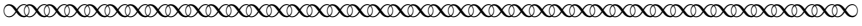
And, finally, the concluding sentence in the argument:



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 37 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 38 Repeat the same division done in Task 36: what is the remainder when we divide $1 \cdot 2 \cdot 3 \cdots (n-1) + 1$ by k?

Task 39 Does the fact that the quantifiers from Task 35 and Task 37 are different present a problem with the argument? Explain why or why not.

Task 40 Explain how your answers to Tasks 36 and 38 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 a 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 41 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?

7 Second Remark: Alternate Proof of Wilson's Theorem

As we've seen, Lagrange used his first proof of Wilson's theorem to also prove Fermat's Little Theorem.[12] He further claimed that this combined approach to proving the two theorems had the advantage of explicitly demonstrating the connection between Wilson's Theorem and Fermat's Little Theorem. Nevertheless, Lagrange gave a second proof that showed Wilson's Theorem as a consequence of Fermat's Little Theorem, which we will work through in this section.

Since we'll start with Fermat's Little Theorem this time, we re-state it first:

Fermat's Little Theorem.
If p is prime and a is relatively prime to p, then p divides $a^{p-1} - 1$.

We also re-state Wilson's Theorem, somewhat more succinctly this time, but still using Lagrange's notation:

Wilson's Theorem.
If n is prime, then n divides $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots (n-1) + 1$.

Lagrange used the "theory of differences" for his 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 $1, 2, 3, \ldots n$ 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

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

[12] That is, Lagrange showed that both Wilson's Theorem and Fermat's Little Theorem follow from a divisibility statement that he derived using coefficients of polynomials.

On the other hand, since the series

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

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 $1, 2, 3, \ldots, n-1$; and thus we'll have the equation

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1) =& n^{n-1} - (n-1)(n-1)^{n-1} + \frac{(n-1)(n-2)}{2}(n-2)^{n-1} \\ & - \frac{(n-1)(n-2)(n-3)}{2 \cdot 3}(n-3)^{n-1} + \ldots + 1. \end{aligned} \tag{9}$$

Task 42 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.

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:

$$1, 16, 81, 256, 625, 1296, \ldots.$$

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

$$15, 65, 175, 369, 671, \ldots.$$

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 43 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}, $3^{n-1}, \ldots$ 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.[13] Lagrange even told us what the constant value is, when he wrote:

> "On the other hand, since the series $1, 2^{n-1}, 3^{n-1}, \ldots$ 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 $1, 2, 3, \ldots, n-1$."

Task 44 Confirm that your computations in Task 43 are correct by checking the fourth difference against the value Lagrange indicated in the quote above.

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

$$1^4,\ 2^4,\ 3^4,\ 4^4,\ 5^4, \ldots.$$

So, the first difference is the sequence

$$2^4 - 1^4\ ,\ \ 3^4 - 2^4\ ,\ \ 4^4 - 3^4\ ,\ \ 5^4 - 4^4\ , \ldots.$$

The second difference, after simplifying, is then the sequence

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

Task 45 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 46 Reconcile your results in Tasks 43 and 45 with the right side of the identity (9), which is restated here for your convenience.

$$\begin{aligned} 1\cdot 2\cdot 3\cdot 4\cdots(n-1) =& n^{n-1} - (n-1)(n-1)^{n-1} + \frac{(n-1)(n-2)}{2}(n-2)^{n-1} \\ & - \frac{(n-1)(n-2)(n-3)}{2\cdot 3}(n-3)^{n-1} + \ldots + 1 \end{aligned} \tag{1}$$

Lagrange would have known the identity (9) from the theory of differences. It appeared in work done by Euler,[14] 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.[15] In what follows, it will be important to remember that n is assumed to be a prime number. Lagrange continued his argument as follows.

[13] For example, Gottfried Leibniz (1646–1716) 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.

[14] The 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.

[15] That is, the identity (9) is true for all values of n, whether they are prime or not.

Suppose now that we divide the second side of this equation [(9)] 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 $(n-1)^{n-1}, (n-2)^{n-1}, \ldots$ will all give a remainder of 1, by the theorem of Mr. Fermat. Thus, putting in the place of these terms their remainders $0, 1, 1, \ldots$ we'll have the total remainder

$$-(n-1) + \frac{(n-1)(n-2)}{2} - \frac{(n-1)(n-2)(n-3)}{2 \cdot 3} + \ldots, \tag{10}$$

or rather

$$(1-1)^{n-1} - 1; \text{ that is, } -1. \tag{11}$$

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.

Task 47 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 48 Explain why "... the terms $(n-1)^{n-1}, (n-2)^{n-1}, \ldots$ 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 again need the **Binomial Theorem**. We re-state here it in the form we need:

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

Task 49 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 50 Assume n is an odd prime. Use this fact to simplify the $(-1)^{n-k}$ factors in your answer to Task 49. Then, identify the part of the resulting expression that Lagrange showed is the remainder (10). Finally, show why the expression for the remainder given in (10) is equivalent to the expression given in (11).

Task 51 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.[16] Show how this, finally, gives the divisibility statement in Wilson's Theorem.

You can make a slight modification to the argument in Task 50 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 52 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.

8 Conclusion

In the first part of this project, we have studied Lagrange's proof of Wilson's Theorem and also Lagrange's demonstration that Fermat's Little Theorem follows from Wilson's Theorem. We then studied Lagrange's proof of the converse of Wilson's Theorem and a second proof given by Lagrange for Wilson's Theorem. We'll conclude with some brief comments about Fermat's Little Theorem, and the importance of both Wilson's and Fermat's Little Theorem to mathematics.

8.1 Fermat and Fermat-Euler

Lagrange was interested in Fermat's Little Theorem, which we re-state here:

> **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 53 Explain why the Fermat-Euler Theorem implies Fermat's Little Theorem.

Fermat stated his theorem in 1640. Euler provided the first published proof in 1736,[17] and 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.[18]

[16] The Division Theorem can be equivalently stated with $-\frac{b}{2} \leq r < \frac{b}{2}$.
[17] Leibniz was aware of Ferma's result even earlier and perhaps had a proof, but didn't publish one.
[18] http://eulerarchive.maa.org/

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

Task 54 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.

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 *Œuveres de Lagrange*, Tome 3, pp. 425–440.

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. It presents Lagrange's proof of Wilson's Theorem. Modern textbooks typically present a proof using Fermat's Little Theorem (If p is prime and a relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.) Lagrange's proof gives Fermat's Little Theorem (aka, the Fermat-Euler Theorem) as a consequence. In his paper, Lagrange went on to prove the converse of Wilson's Theorem. He also provided a second proof of Wilson's Theorem (starting from Fermat's Little Theorem). All of these results are treated in this project. There are also three projects which treat the results independent, each available at https://digitalcommons.ursinus.edu/triumphs_number:

- *Lagrange's Proof Wilson's Theorem — and More!* (2–3 days)
  Gives Lagrange's first proof and the implication of Fermat's Little Theorem.
- *Lagrange's Proof of the Converse of Wilson's Thoerem* (1 day)
  Gives Lagrange's proof of the converse to Wilson's Theorem.
- *Lagrange's Alternate Proof of Wilson's Theorem* (1–2 days)
  Gives Lagrange's second proof of Wilson's Theorem.

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 $n|a+b$ and $n|a$, then $n|b$) are used a couple times. Euclid's Lemma (i.e., a prime divisor of a product must divide one of its factors) is used once (in Task 18). The Division Theorem is useful in two 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. Perhaps, the argument most unfamiliar to students is for Task 28. The Binomial Theorem is needed, but stated in the text 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 introduced after Lagrange. In the converse section, 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

Following a short historical introduction, Section 1 presents Lagrange's statement of Wilson's Theorem. Sections 2–4 then develop Lagrange's proof of that theorem. Section 5 gives the demonstration of how Lagrange's proof of Wilson's Theorem also gives a proof of Fermat's Little Theorem as a consequence. Section 6 presents Lagrange's proof of the converse to Wilson's Theorem. Section 7 presents an alternate proof of Wilson's Theorem as a consequence of Fermat's Little Theorem. The Conclusion in Section 8 summarizes Lagrange's work on Wilson's Theorem.

Lagrange's work is relatively easy to read and he provided a good amount of detail. Many of the tasks require short answers. Students primarily need to carefully read Lagrange's argument and fill in a few "missing lines." A few tasks ask students to compute examples. These computations

aren't strictly necessary. To save time, you could skip them, present and discuss the computations, or assign them as homework.

The section on the converse of Wilson's Theorem is quick. It provides good practice for using quantifies and proof techniques. The possibility of using the converse of Wilson's Theorem as a primality test is briefly discussed towards the end of this section.

The section with the alternate proof starts from Fermat's Little Theorem and uses the "theory of differences." Students need to think carefully about the identity (9) that Lagrange used here. This proof also illustrates a common technique: expanding $(1-1)^n$.

Some task-by-task commentary follows.

- Task 4: I would emphasis to students they are **the same** As.
- Task 6: The solution to this task is revealed in the subsequent Lagrange excerpt. You might want to print the project so that you can hand out that excerpt after students complete this task.
- Task 8: This task and Tasks 10 and 11 go together. As mentioned below, you could skip, present, or assign these two tasks as homework to save time. I think it helps to get your hands dirty to understand what's happening.
- Task 10: If you assign this task as homework, you need to tell students whether they should solve by comparing coefficients or use (5). If you have students complete this task during class, don't hand out the next page until they have finished.
- Task 11: This task only makes sense if you do Tasks 8 and 10.
- Task 19: This task may be confusing if students wrote a "simplified" answer for Task 13. The unsimplified expression may appear in their answer to Task 12.
- Task 20: I wouldn't worry about a formal inductive proof for this task.
- Task 21: Here is Lagrange's solution:

…that the number $A^{(n-1)}$ being augmented by one will be divisible by n; because the formula which will serve to determine its value will be

$$(n-1)A^{(n-1)} = \frac{n(n-1)(n-2)\cdots 1}{1\cdot 2\cdot 3\cdots n} + \frac{(n-1)(n-2)\cdots 1}{1\cdot 2\cdots(n-1)}A' + \frac{(n-2)(n-3)\cdots 1}{1\cdot 2\cdots(n-2)}A'' + \ldots,$$

that is

$$(n-1)A^{(n-1)} = 1 + A' + A'' + A''' + \cdots + A^{(n-1)};$$

thus

$$A^{(n-1)} + 1 = nA^{(n-1)} - A' - A'' - A''' - \cdots - A^{(n-2)};$$

thus since $A', A'', \ldots, A^{(n-2)}$ will all be divisible by n, it follows that $A^{(n-1)} + 1$ will always be divisible by 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. At the end of a class day assign the next couple tasks for homework if those next tasks are good ones for students on their own.

Possible Modifications of the PSP

- To save time you might include the computation answers to Tasks 8 and 10 in the PSP handout and present/discuss them in class rather than ask students to do the computations.
- The proof of Wilson's Theorem ends with Task 22 at the end of Section 4 (The Main Theorem). Section 5 (A Second Corollary) shows that Fermat's Little Theorem follows from Lagrange's proof of Wilson's Theorem. This section is optional. If it is not covered, the subsequent sections, including the Conclusion, can be read independently.
- I have not tried this, but rather than dedicating full days to the project you could interweave it with a textbook section on divisibility. This would allow more flexibility for assigning good tasks (computation oriented, etc.) as homework.

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)

- **Day One Preparation:** As homework before the first class day, students read up to Task 2 and answer Tasks 1–3.
- **Day One:** Work from Task 4 to Task 15. Most tasks require only short answers. Tasks 8 and 10, however, involve computation. You may want to present and discuss the computations requested here. Neither is strictly needed for the development of the proof but it's hard to understand what's going on without getting your hands a little dirty.
- **Day Two Preparation:** Any of the Tasks 4 to 15 not completed during class time. Read the excerpt that follows Task 15 and complete Tasks 16 and 17.
- **Day Two:** Work from Task 18 to Task 22. As noted earlier, instructors who decide to end the PSP with Section 4 (Lagrange's proof of Wilson's Theorem) could also have students read Section 6 (Conclusion) at this point, perhaps as homework.
- **Day Three Preparation:** Ask students to read the statement of Fermat's Little Theorem and provide several numerical examples that illustrate the theorem.
- **Day Three:** Tasks 23 to 29 in Section 5 (Lagrange's proof of Fermat's Little Theorem.)
- **Day Four preparation:** Assign Tasks 30 to 32 as homework.
- **Day Four:** Tasks 33 through 40. Assign Task 41 as homework.
- **Day Five preparation:** Read the first part of Section 7 and complete Tasks 42 through 44.
- **Day Five:** Task 45 through 52.
- **Wrap-up** Ask students to read the conclusion an complete Tasks 53 and 54.

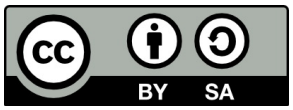
Connections to other Primary Source Projects

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)
- *Lagrange's Proof of the Converse of Wilson's Thoerem*, Carl Lienert (1 day)
- *Lagrange's Alternate Proof of Wilson's Theorem*, Carl Lienert (1–2 days)
- *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/.