Ursinus College

Digital Commons @ Ursinus College

Summer 2017

Primes, Divisibility, and Factoring

Dominic Klyve
Central Washington University, Dominic.Klyve@cwu.edu

Recommended Citation

Primes, Divisibility, and Factoring

Dominic Klyve*

June 21, 2021

1 Introduction

In 1732, Leonhard Euler (1707–1783) was 25 years old. After five years working in St. Petersburg, Russia, he had finally gotten the job he had long wanted — Mathematics Professor at the Science Academy. Perhaps to celebrate his new position, he started reading a set of letters about integers and primes that Pierre de Fermat (1607–1665) had written to other mathematicians a century early. As he read, Euler realized that he had some new ideas of his own. He had never before written about the integers, but he was fairly excited about what he found. On September 26 of that year, he read a short five-page article about his findings, [Euler, 1738], filled with powerful new insights into the nature of integers and primes, to the rest of the academy. His article, "Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus" ("Observations on a theorem of Fermat and others concerned with prime numbers"), would determine much of the work he would pursue in number theory for the next decade. There is no record that anyone was excited at the time — the academy didn't even publish his paper for five years.

Nevertheless this paper, containing several statements that Euler couldn't even prove, and which nobody seemed to care about, would one day become a pillar of public-key cryptography, the system which now protects billions of dollars sent over the internet every day.

This project will lead you through Euler's work. By the time you are done reading his paper and answering the enclosed questions, you will have a good grounding in elementary number theory. After you finish it, you will also have the chance to prove several theorems which stumped even Euler!

2 Fermat Primes

Let us begin with just the first paragraph of Euler's paper, to see how he began.[1]

---

*Department of Mathematics, Central Washington University, Ellensburg, WA 98926; `dominic.klyve@cwu.edu`.

[1]All Euler translations, unless otherwise noted, were prepared by Jordan Bell (University of Toronto), 2008. The full text of that translation appears in Appendix II of this project for those who wish to read Euler's paper without interruptions. A scan of the original Latin paper also appears in Appendix III.
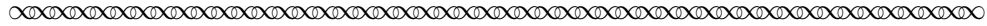
It is known that the quantity $a^n + 1$ always has divisors whenever n is an odd number or is divisible by an odd number aside from unity. Namely $a^{2m+1} + 1$ can be divided by $a + 1$ and $a^{p(2m+1)} + 1$ by $a^p + 1$, for whatever number is substituted in place of a. But on the other hand, if n is a number which is divisible by no odd number aside from unity, which happens when n is a power of two, no divisor of the number $a^n + 1$ can be assigned. So if there are prime numbers of this form $a^n + 1$, they must all necessarily be included in the form $a^{2^m} + 1$. But it cannot however be concluded from this that $a^{2^m} + 1$ always exhibits a prime number for any a; for it is clear first that if a is an odd number, this form will have the divisor 2.
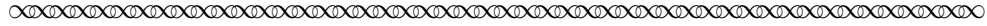
Wow! This is a lot to take in at once. There are a lot of statements here which, though they may not be mathematically deep, are far from obvious at first reading. Let's work through the paragraph one piece at a time. Euler's first sentence made a claim about the divisors of some positive integers. Read it again:
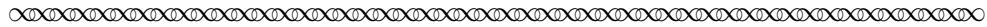
It is known that the quantity $a^n + 1$ always has divisors whenever n is an odd number or is divisible by an odd number aside from unity.
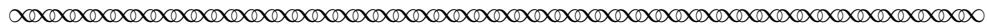
Task 1 What is unity? Find all n up to 16 (other than unity) for which n is an odd number or is divisible by an odd number. How else could you describe this class of numbers?

Task 2 Euler's statement that $a^n + 1$ has divisors may seem unusual — every number has divisors. What do you think he meant here? (Hint: what Euler called "divisors" are sometime called "non-trivial divisors" today.)

Task 3 Now let $a = 2$. Check whether Euler's claim in the first sentence is true for all appropriate n less than 8. Was he correct in this case? What do you notice about the non-trivial divisors of $2^n + 1$ when n is odd?

Task 4 Now let $a = 3$. Once again, verify the first sentence for all appropriate n up to $n = 5$. What do you notice about the non-trivial divisors of $3^n + 1$?

Task 5 Formulate a conjecture about how to find a non-trivial divisor of $a^n + 1$ for any a when n is an odd number other than unity or is divisible by an odd number other than unity.

Euler himself made a claim about divisors of $a^n + 1$ in the second sentence of the paper. He claimed
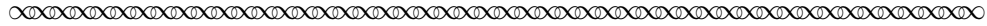
Namely $a^{2m+1} + 1$ can be divided by $a + 1$ and $a^{p(2m+1)} + 1$ by $a^p + 1$, for whatever number is substituted in place of a.
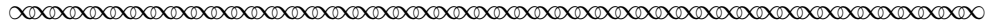
You have already verified this for $a = 2$ and $a = 3$ in Tasks 3 and 4 above. We would, however, like to establish this claim for all values of a.

Task 6   Find an algebraic proof that $a^{2m+1} + 1$ can be divided by $a + 1$. (If this seems too difficult, try it first for the cases $m = 0$, $m = 1$, and $m = 2$. Use the patterns that you find to give you a hint about what to try in the general case.)
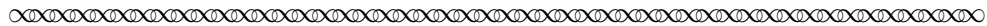
Task 7   Euler also claimed that $a^n + 1$ has a non-trivial divisor not just when n is odd, but when n is divisible by an odd number. Modify your proof in Task 6 to show that $a^{p(2m+1)} + 1$ is divisible by $a^p + 1$.

After describing what happens when the exponent is odd or a multiple of an odd number, Euler continued:

But on the other hand, if n is a number which is divisible by no odd number aside from unity, which happens when n is a power of two, no divisor of the number $a^n + 1$ can be assigned.
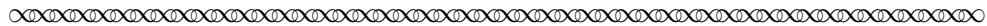
Task 8   What did Euler seem to be claiming about numbers of the form $a^{2^n} + 1$? Was he right? Try a few small values of a and n, and see if you can make sense of this claim.

In fact, if we read on, we see that Euler was quite aware that $a^{2^n} + 1$ was not always prime. In the next paragraph of his paper, he gave several examples.
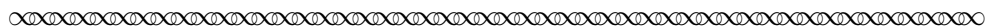
Then also, even if a denotes an even number, innumerable cases can still be given in which a composite number results. For instance, the formula $a^2 + 1$ can be divided by 5 whenever $a = 5b \pm 3$, and $30^2 + 1$ can be divided by 17, and $50^2 + 1$ by 41. Similarly, $10^4 + 1$ has the divisor 73, $6^8 + 1$ has the divisor 17, and $6^{128} + 1$ is divisible by 257.
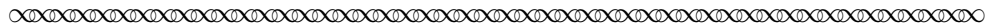
Perhaps the most striking thing about this to Euler's contemporaries — and to many modern readers — is the ease with which Euler worked with big numbers. You can check for yourself that $50^2 + 1$ is divisible by 41. But $6^8 = 1679616$. Checking (let alone finding) that 17 is a factor of $6^8 + 1$ would have been difficult in the era before electronic calculators. Even more boggling is the claim that $6^{128} + 1$ is divisible by 257.

Task 9   (a) Verify Euler's numerical claims in this paragraph about divisors of the quantity $a^{2n} + 1$. (

(b) The value $6^{128} + 1$ is quite large. Calculate it (probably using a computer). How do you think Euler could have discovered this was divisible by 257, given that he lived long before computers and calculators?

Euler's last claim in the paragraph above seems quite interesting. Recall that he claimed
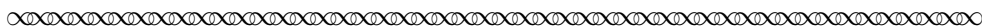
⊗⊗⊗

Yet no case has been found where any divisor of this form $2^{2^m} + 1$ occurs, however far we have checked in the table of prime numbers, which indeed does not extend beyond 100000.

⊗⊗⊗

If no divisors of $2^{2^m} + 1$ can be found, of course, then numbers of the form $2^{2^m} + 1$ are always prime. Let's check whether this could be true.
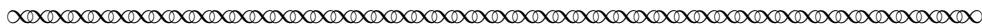
Task 10   Make a table with three columns. In the first, list the first few small integers $m = 0, 1, 2, \ldots$, until you feel like stopping. In the second column, compute $2^{2^m} + 1$. Test whether these numbers are prime, and record the answer for each in the third column. State a conjecture about numbers of this form.

Task 11   It seems that when Euler checked if a number was prime, he used tables of prime numbers. Check your textbook to see if you have one, or look online. Do these tables help you with the previous problem? If so, in what way? If not, why not?

Depending on what you conjectured in the last question, you may find that your conjecture matches that of another great mathematician, as Euler stated next:
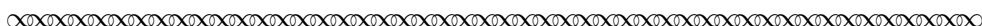
⊗⊗⊗

For this and perhaps other reasons, Fermat was led to state there to be no doubt that $2^{2^m} + 1$ is always a prime number, and proposed this eminent theorem to Wallis and other English Mathematicians for demonstration. Indeed he admitted to not himself have a demonstration of this, but did not however hold it to be any less than completely true. He also praised the great utility of this, by means of which one can easily exhibit a prime number larger than any given number, which without a universal theorem of this type would be very difficult.

⊗⊗⊗
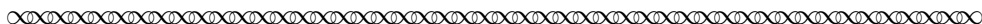
When Fermat "'proposed this eminent theorem to …other …mathematicians for demonstration," he was challenging them to prove the fact. It seems that Fermat couldn't prove the theorem himself, but he still held it to be "completely true."

Task 12   Do you think it is appropriate for a mathematician to hold a statement to be "completely true," even if it doesn't have a proof? Why or why not?

Task 13 Fermat claimed that if $2^{2^m}+1$ is prime, "one can easily exhibit a prime number larger than any given number." How large would m have to be for $2^{2^m}+1$ to be bigger than a million? Bigger than a trillion? Bigger than 10^{100}?

In fact, at the time that Euler wrote this paper, the claim that $2^{2^m}+1$ is always prime seems to have been widely believed. Not only had nobody found a counterexample, but the truth of the statement was asserted by the great Fermat himself. Mathematicians had known since the time of Euclid that there were infinitely many prime numbers; after they accepted the claim of Fermat, they believed they could go one step farther, and could easily write down prime numbers as large as they wanted. In this context, Euler's next paragraph would have been quite shocking to mathematicians of his day:

∞∞

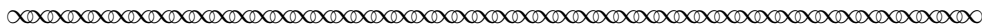The truth of this theorem can be seen, as I have already said, if one takes $1, 2, 3$ and 4 for m; for these yield the numbers $5, 17, 257$ and 65537, which all occur among the prime numbers in the table. But I do not know by what fate it turned out that the number immediately following, $2^{2^5}+1$, ceases to be a prime number; for I have observed after thinking about this for many days that this number can be divided by 641, which can be seen at once by anyone who cares to check. For it is $2^{2^5}+1 = 2^{32}+1 = 4294967297$. From this it can be understood that the theorem fails in this and even in other cases which follow, and hence the problem of finding a prime number greater than a given number still remains unsolved.

∞∞
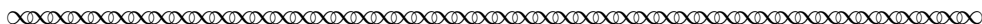
It is not clear from the text precisely how Euler's several days of thinking helped him solve this problem, but it is easy to verify the answer.

Task 14 Check, either by hand or with a calculator, that $2^{2^5}+1$ is divisible by 641. Give another factor of $2^{2^5}+1$.

We can get some insight into Euler's thoughts by looking for specific integer values that are never divisors of $2^{2^m}+1$, no matter what value we give to m. For example, it turns out that for $m > 0$, $2^{2^m}+1$ is always 2 more than a multiple of 3. In fact, $2^{2^m}+1$ is never divisible by $3, 5$, or 7, as you can show by mathematical induction (if you have learned that technique) in the following tasks.

Task 15 Use an induction argument to show that for $m > 0, 2^{2^m}+1-2$ is always divisible by 3. (That is, show that $2^{2^m}+1 \equiv 2 \pmod 3$.)

Task 16 Use an induction argument to show that for $m > 1, 2^{2^m}+1$ is never divisible by 5.

Task 17 Now try using induction to show that $2^{2^m}+1$ is never divisible by 7. (This is a bit trickier, but it's not too hard.)

By using arguments like this, Euler reduced the number of factors of these special numbers he would have needed to check by hand. In fact, he had discovered a secret trick to help him, which he wouldn't reveal for several more years. His trick wasn't strong enough, though, to help him decide whether $2^{2^6}+1$ is prime.

Numbers of the form $2^{2^n} + 1$ are today called *Fermat numbers*; if a Fermat number is prime, we call it a *Fermat prime*. In order to simplify our notation, we will denote these Fermat numbers as $F_m = 2^{2^m} + 1$. We have established so far that F_0, F_1, F_2, F_3, and F_4 are prime, but F_5 is composite. This is often used as an example for why we require mathematical proofs of statements, and don't trust patterns. Let's say we wanted to check the primality of F_6. How hard would this be?

Task 18 How many digits are in F_6? See if a computer can test whether it's prime. If it's not, try to find a factor of it. Can a computer check F_7? F_8? F_9? Try this, and report what you find.

Task 19 Now look up modern results about Fermat numbers. Which ones have been proved to be prime, and which composite? How close was Fermat to being correct when he claimed that F_n is prime for all n?

Euler, however, didn't discuss his methods in his paper, nor did he pursue these questions about Fermat numbers. Instead, he quickly shifted his focus to another kind of prime number.

3 Perfect Numbers

As we know, by the time that Euler presented this paper, he had been in St. Petersburg for five years. This, it turns out, was long enough to discover that he didn't respect all his colleagues. One of these was the philosopher Christian Wolff (1679–1754). Wolff was probably the most famous philosopher in Europe at this time. He had taken the leadership among the philosophers of continental Europe after the death of Gottfried Leibniz (1646–1716). Over the next decades, Wolff wrote hundreds of essays about everything from philosophy and physics to farming and theology.

Euler had first come into contact with Christian Wolff a few years before writing his 1738 paper, when he stopped to visit Wolff in Marburg during his move from Switzerland to St. Petersburg. We don't know whether it was at this meeting or later that the two scholars began their dispute, but we do know that Euler was strongly opposed to Wolff's philosophy, and he seemed eager for a chance to show the world that Wolff was not quite so smart as many people seemed to believe.

So what did Euler do? In the middle of his paper about prime numbers and factors, he digressed for a bit to point out recent errors Wolff had made in mathematics. Perhaps fortunately, this tradition seems to have vanished from modern mathematics. You can probably search your course textbook for days without finding an example of one scholar insulting another.[2]

---

[2]To be fair to Euler, we should note that this was not typical of his writing over his long career. He was almost always generous, gracious, and quick to praise the work of others.
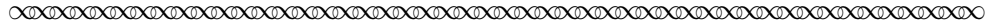
$\infty\!\infty$

I will now examine also the formula $2^n - 1$, which, whenever n is not a prime number, has divisors, and this is true not only for $2^n - 1$, but also for $a^n - 1$. But if n is a prime number, it might seem that $2^n - 1$ also always gives a prime; this however no one, as far as I know, has dared to profess, and indeed it can easily be refuted. Namely $2^{11} - 1$, i.e. 2047, has the divisors 23 and 89, and $2^{23} - 1$ can be divided by 47. I see also that the Celebrated Wolff has not only not mentioned this in the new edition of his *Elem. Matheseos*, where he investigates the perfect numbers and includes 2047 among the primes, but also has 511 or $2^9 - 1$ as a prime, while it is divisible by $2^3 - 1$, i.e. 7. He also gives that $2^{n-1}(2^n - 1)$ is a perfect number whenever $2^n - 1$ is prime; therefore n must also be a prime number.

$\infty\!\infty$
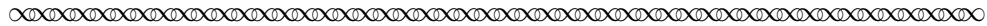
Task 20 Note that Euler's first claim is that $2^n - 1$ always has factors if n is not prime. Prove that this is true algebraically by finding a factor of $2^n - 1$ for an arbitrary composite n. (It may be helpful to write n as the product $n = mk$ of two natural numbers m and k both greater than 1.)

Task 21 Euler then pointed out that even if n is prime, $2^n - 1$ may not be prime. Identify the two specific values of n for which $2^n - 1$ is composite mentioned by Euler. Then try to find another such n. (This is tricky, and almost certainly requires a computer. If you haven't been using software for working with large numbers in your course, note that it's easy to check these factorizations on the internet. Go to `www.wolframalpha.com`, and try entering "is $2^{11} - 1$ prime?").

At the end of the excerpt above, Euler mentioned perfect numbers. A *perfect number* is an integer which is equal to the sum of its proper divisors. For example, the proper divisors of 6 are $1, 2$, and 3, and $1 + 2 + 3 = 6$, so 6 is a perfect number.

Task 22 Find the next perfect number after 6.

Task 23 If $2^n - 1$ is prime, it's possible to write down (in terms of n) all of the factors of $2^{n-1}(2^n - 1)$. For example, if $n = 5$, then $2^{n-1}(2^n - 1) = 2^4(2^5 - 1)$, which has the following ten factors:

$$1 \ , \ 2 \ , \ 2^2 \ , \ 2^3 \ , \ 2^4 \ , \ (2^5 - 1) \ , \ 2(2^5 - 1) \ , \ 2^2(2^5 - 1) \ , \ 2^3(2^5 - 1) \ , \ 2^4(2^5 - 1)$$

(a) Check that $2^4(2^5 - 1)$ is a perfect number by finding the sum of its proper divisors. Do this without actually computing the numerical value of each factor.

(b) Now let n be arbitrary, and assume that $2^n - 1$ is prime. Write down (in terms of n) all of the factors of $2^{n-1}(2^n - 1)$. (It's okay to use '...' here!) Then sum the proper factors of $2^{n-1}(2^n - 1)$ to check Euler's claim that $2^{n-1}(2^n - 1)$ is a perfect number whenever $2^n - 1$ is prime.

The last sentence in Euler's excerpt above is in fact very old. Let's compare it to a text written two thousand years earlier, by Euclid (c. 365–300 BCE). Euclid wrote a work of 13 books, today called the *Elements*. The books are most famous today for the results they contain about geometry, but there are

also many results about proportions and the theory of numbers. In fact, Proposition 36 of Book IX very closely corresponds to what Euler just claimed. Euclid, however, expressed himself rather differently. His statement of the proposition is as follows:
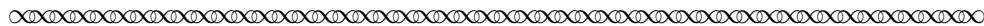
∞∞∞

If as many numbers as we please beginning from a unit be set out continuously in double proportion, until the sum of all becomes prime, and if the sum multiplied into the last make some number, the product will be perfect.   Euclid, IX.36

∞∞∞
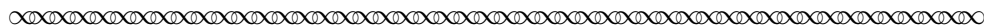
This sounds a little bit confusing at first reading. Go back and read it again, slowly.

Task 24 What did Euclid mean by "'If as many numbers as we please beginning from a unit be set out continuously in double proportion"? Give an example of a sequence of numbers set out in double proportion.

Task 25 Euclid was interested in the sum of the numbers in double proportion. If we write out k numbers beginning with a unit in double proportion, what is their sum?

Task 26 What did Euclid mean by "the last"?

Task 27 Write Euclid's proposition in modern symbolic notation. How does it compare to Euler's statement about perfect numbers?

4 Mersenne and Sophie Germain Primes

Let us now return to Euler's paper. In section 1 of this project, we carefully examined certain numbers of the form $2^n + 1$ (as a special case of numbers of the form $a^n + 1$). In section 2, we then found that numbers of the form $2^n - 1$ are helpful for finding perfect numbers. In particular, if $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is a perfect number. We now follow Euler in considering more closely numbers of the form $2^n - 1$. Today we name these numbers for Marin Mersenne (1588–1648), a seventeenth-century Catholic priest who wrote about numbers of this form. At the time that Euler wrote his paper, he seemed to have been unaware of Mersenne's work, and made no mention of him.

We know from Euler's earlier discussion that $2^n - 1$ is always composite if n is composite. (You gave a proof of this in Task 20.) What about the cases where n is prime? For which of these is $2^n - 1$ prime? It would be easier not to check them all individually, so Euler started to look for some cases which can be ruled out immediately.
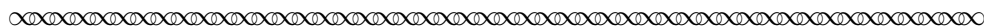
∞∞∞

I have found it a worthwhile effort to examine those cases in which $2^n - 1$ is not a prime number while n is. I have also found that if $n = 4m - 1$ and $8m - 1$ are prime numbers, then $2^n - 1$ can always be divided by $8m - 1$. Hence the following cases should be excluded: 11, 23, 83, 131, 179, 191, 239 etc., which numbers when substituted for n yield $2^n - 1$ that is a composite number.

∞∞∞
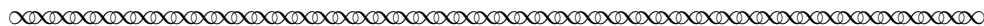
Task 28 Look at Euler's claim that $2^{4m-1} - 1$ is divisible by $8m - 1$ in certain cases.

    (a) Check whether $2^{4m-1} - 1$ is divisible by $8m - 1$ when $m = 1, 2$, and 3.

    (b) If there is a value of m for which $8m - 1$ does not divide $2^{4m-1} - 1$, does this contradict Euler's claim? Explain why or why not.

In this last excerpt, Euler was interested in primes $p = 4m - 1$ for which $8m - 1$ is also prime. Let p be such a prime. It is then easy to verify that $2p + 1 = 8m - 1$. *(Make sure you do this!)* In other words, Euler was interested in primes p of a particular form for which $2p + 1$ is also prime. Today, any prime p for which $2p + 1$ is also prime is called a *Sophie Germain prime*. These primes are of interest to number theorists for many reasons. One is that a brilliant mathematician named Sophie Germain[3] (1776–1831) used these primes (and others) when she tried to prove Fermat's Last Theorem (yes — named for the same Fermat!).

Task 29 In the previous excerpt, Euler listed seven primes p that he claimed are Sophie Germain primes.

    (a) Verify that he was correct. Then find a Sophie Germain prime p for which $2p + 1$ is also a Sophie Germain prime.

You now have a (short) chain of primes, each of which is one more than twice the last.

    (b) See if you can find a longer chain of such primes. (At the time this project was written, the longest such chain ever discovered had 17 primes — can you do better?)

Task 30 (a) Do you think there are infinitely many Sophie Germain primes?

    (b) What evidence or heuristic reasoning can you give for this?

Euler wasn't thinking about Sophie Germain primes when he wrote his 1732 number theory paper. He was just trying to figure out for which primes p he could be sure that $2^p - 1$ was composite.[4] Euler listed some of these (the Sophie Germain primes of form $4m - 1$) in the previous excerpt. He then set out to find others:
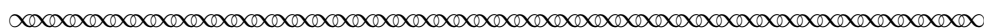
⊗⊗⊗

    Neither however can all the remaining prime numbers be successfully put in place of n, but still more must be removed; thus I have observed that $2^{37} - 1$ can be divided by 223, $2^{43} - 1$ by 431, $2^{29} - 1$ by 1103, $2^{73} - 1$ by 439; however it is not in our power to exclude them all. Still, I venture to assert that except for those cases noted, all prime numbers less than 50 and perhaps even 100 yield $2^{n-1}(2^n - 1)$ which is a perfect number, thus 11 perfect numbers arise from the following numbers taken for n, 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47.

⊗⊗⊗

---
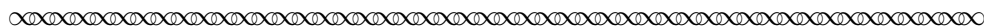
[3]Sophie Germain's story is fascinating — check out *Sophie Germain: Revolutionary Mathematician* by Dora E. Musielak (Springer, 2020) to learn more!

[4]Remember that Euler was really interested in primes p for which $2^p - 1$ is prime, since in that case $2^{p-1}(2^p - 1)$ will be a perfect number. But if he could categorize primes p for which $2^p - 1$ is composite, then he was able to immediately rule out some cases.

Combining Euler's comments in the previous two excerpts, note that he eliminated the following specific primes p from the list of primes for which $2^p - 1$ can be prime:

$$11, 23, 29, 37, 43, 73, 83, 131, 179, 191, 239$$

He then "ventured to assert" that, for each of the remaining primes p less than 50, the number $2^{p-1}(2^p - 1)$ is a perfect number; in other words, that $2^p - 1$ is prime for each of the following values of p:

$$2, 3, 5, 7, 13, 17, 19, 31, 41, 47$$

There is quite a long tradition in mathematics of scholars trying to predict which values of p will generate prime numbers of the form $2^p - 1$. The most famous set of such conjectures is due to Mersenne, but several other scholars (including Leibniz, who co-invented calculus) tried too. All of these earlier thinkers missed some guesses — they were wrong sometimes. We might wonder whether Euler did any better.

Task 31 Check (using a computer) Euler's conjecture that $2^p - 1$ is prime for each of the primes listed at the end of the passage above: 2, 3, 5, 7, 13, 17, 19, 31, 41, 47. (One easy way to do this is to type things like "Is $2^{13} - 1$ prime?" at `www.wolframalpha.com`.) For which of these was Euler correct?

One of the most puzzling things about the passage above is how Euler came up with these factors. The value of $2^{73} - 1$ is the whopping $9,444,732,965,739,290,427,391$. Finding a factor of such a number is no easy task, and yet Euler was right in his assertion that $2^{73} - 1$ is divisible by 439. Earlier, Euler left us in the dark as to how he found a factor of $2^{2^5} + 1$, but at this point he decided to be more generous. He next shared with his readers the ideas which led him to find these factors.

5   Toward the Euler-Fermat Theorem

Euler continued his paper:
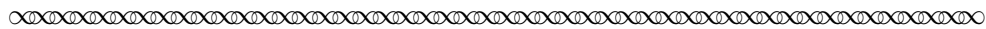
⚬⚬⚬

I have deduced these observations from a not inelegant theorem, whose proof I do not have, but indeed of whose truth I am completely certain. This theorem is: $a^n - b^n$ *can always be divided by* $n + 1$*, if* $n + 1$ *is any prime number which divides neither* a *nor* b; I believe this demonstration is more difficult because it is not true unless $n + 1$ is a prime number.

⚬⚬⚬
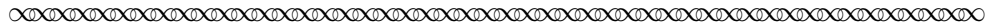
This theorem is an important part of the remainder of the project — from now on we'll refer to it as "Euler's Theorem." Euler's Theorem is quite amazing, and it is the first step toward some very powerful ideas which he would develop over the next decades. Let's first make sure we understand what this theorem is saying.

The theorem first requires that $n + 1$ be prime. If we choose $n = 2$, say, this hypothesis is satisfied. In this case, the theorem claims that $a^2 - b^2$ will always be divisible by 3, as long as a and b are not divisible by 3.

Task 32 Choose a few permissible a and b to test Euler's Theorem in the case that $n = 2$.

Task 33 If we set $n = 1$, the hypothesis of the theorem seems to hold — after all, $1 + 1$ is prime! What does the theorem claim in this case? Is it correct?

Task 34 Now choose another value of n that satisfies the hypothesis of the theorem. Put this result in English, as we did above for the case of $n = 2$. Choose a few permissible a and b to test the theorem again.

Task 35 Euler claimed that this is a theorem, but that he did not have a proof of it. This is the second time in the paper he discussed an unproven claim, but this time he was reporting his own belief (rather than Fermat's). Do you think something without a proof should be called a theorem? Why or why not?

Task 36 At the end of the excerpt, Euler wrote "I believe this demonstration is more difficult because it is not true unless $n + 1$ is a prime number." Why might Euler have thought that it would be more difficult to prove a theorem that is only true for prime numbers? Do you agree with him? Why or why not?

The fact that Euler could not prove the "theorem" at the time he wrote this paper makes us think that it might be difficult to prove. It's not too difficult, however, to do this in a few special cases.

Task 37 Prove Euler's Theorem when $n = 2$.

Task 38 Prove Euler's Theorem when $n = 4$.

If you can do this without any further hints, do so!
If you're having trouble, try answering the questions below:

(a) Write down Euler's Theorem when $n = 4$.

The rest of this proof outline will lead us to a proof of the following fact:

FACT:
Starting with any integer that is not divisible by 5, when we divide the 4th power of that integer by 5, we will always get the same remainder.

(b) Explain why this fact (once we prove it!) will be enough to prove Euler's Theorem for $n = 4$ which you stated in part (a) of this task.

(c) For the integers $a = 1, 2, 3, 4$ make a list of the remainders of a^4 divided by 5.
(If you know modular arithmetic, write the values of $a^4 \pmod 5$.)

(d) To show that every integer a (except those divisible by 5) gives the same remainder when we divide a^4 by 5, how many integers a would you actually have to check? Have you already checked them? Explain.

(e) Now put these ideas together to prove Euler's Theorem for $n = 4$.

We're starting to get some insight into what was really going on in Euler's mind. If you're feeling brave, consider trying the next (optional) problem:

Task 39 Prove Euler's Theorem that $a^n - b^n$ can always be divided by $n + 1$, if $n + 1$ is a prime number which divides neither a or b.

This theorem today brings to mind another theorem which appears in all beginning number theory books about primes, powers, and remainders. It's more commonly known as "Fermat's Little Theorem," and can be stated as follows:

Fermat's Little Theorem
For any prime p, and any integer a that is not divisible by p, $a^{p-1} - 1$ is divisible by p.

Mathematicians often like to check whether two theorems are *equivalent*. This means roughly that if we start by assuming either one of them, we should be able to prove the other. We're now going to try to prove that Euler's Theorem is equivalent to Fermat's Little Theorem.

Task 40 By choosing appropriate values of p and b, prove that Euler's Theorem implies Fermat's Little Theorem.

Task 41 Now prove that Fermat's Little Theorem implies Euler's Theorem.

Task 42 Think about what you have done in Tasks 38 and 39 above. Have you proven that Euler's Theorem is true? Explain.

Although Euler didn't mention this in his paper, it is likely that Euler's Theorem was the secret to how he was able, "after thinking about this for many days," to discover that 641 is a factor of Fermat's false prime $2^{2^5} + 1$. You can learn more about this by taking a look at the optional Tasks in Appendix I: Peering into Euler's Mystery. Of course, Euler did tell his readers that he wasn't able to prove his "theorem" when he wrote this paper in 1732. Later he would prove it, and go on to prove a powerful generalization of it (now called the Euler-Fermat theorem), in one of almost a hundred papers he would publish in number theory.[5] Despite his inability to prove it in 1732, Euler was so sure that it was true that he started to apply it to derive other statements.
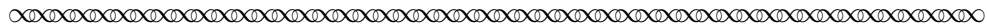
〜〜

From this theorem, it follows at once that $2^n - 1$ can always be divided by $n + 1$ if $n + 1$ is a prime number, or, since each prime aside from 2 is odd, and as when $a = 2$, that case does not happen because of the conditions of the theorem, $2^{2m} - 1$ will always be able to be divided by $2m + 1$, if $2m + 1$ is a prime number. Hence either $2^m + 1$ or $2^m - 1$ will be able to be divided by $2m + 1$.

〜〜

---
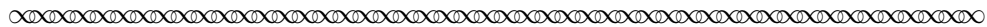
[5]The full Euler-Fermat theorem states that, for any relatively prime integers a and n, $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is the number of integers less than n that are relatively prime to n.

Mathematicians have a habit of sometimes stating that a certain conclusion is very simple, and the reader may not always agree. If a mathematician like Euler says that something "follows at once," then it probably does — once we look at the problem the right way. Sometimes it can be difficult to do this, however, and it's worth paying attention to statements like this, if only as a measure of how well we've been following the arguments.

Task 43 Let's examine this section more closely:

(a) Explain why it "follows at once" from Euler's Theorem that $2^n - 1$ can be divided by $n + 1$ if $n + 1$ is prime (provided $n > 1$). *(Do you see why the fact that $2^n - 1$ is not divisible by $n + 1$ in the case of $n = 1$ does not violate Euler's Theorem?)*

(b) Explain why $2^{2m} - 1$ is always divisible by $2m + 1$ if $2m + 1$ is prime.

(c) For Euler's last claim, that either $2^m + 1$ or $2^m - 1$ is divisible by $2m + 1$, it's not entirely clear at first reading whether this holds for all m, or only those for which $2m + 1$ is prime. Determine which of these is the case by testing this particular claim with some values of m. Based on what you find, rewrite Euler's claim more clearly.

(d) Now prove Euler's claim that either $2^m + 1$ or $2^m - 1$ is divisible by $2m + 1$ (for those m that you decided it should hold in part (c) above).

(e) Now prove the following generalization of Euler's claim:

If $2m + 1$ a prime number that does not divide either a or b,
then either $a^m - b^m$ or $a^m + b^m$ is divisible by $2m + 1$.

At this point, Euler has claimed that when $2m + 1$ is prime, either $2^m - 1$ or $2^m + 1$ is divisible by $2m + 1$. This isn't fully satisfying, though — we might further ask if there is a way to determine when it is $2^m - 1$ that is divisible by $2m + 1$, and when is it $2^m + 1$. Euler would have approached this question the same way many number theorists have through the centuries, by gathering data in the hope of finding a conjecture.

m	$2m + 1$	prime?	which?
1	3	yes	$2^m + 1$
2	5	yes	$2^m + 1$
3	7	yes	$2^m - 1$
4	9	no	n/a

Take time to understand what's going on in this table — it should look like an attempt to figure out in which category each m lands (for those m for which $2m + 1$ is prime).

Task 44 Extend this table until you see a pattern (probably at least until $m = 12$). When you do, formulate a conjecture. It should have the form:

" $2^m + 1$ is divisible by $2m + 1$ if _____ ,
while $2^m - 1$ is divisible by $2m + 1$ if _____ . "

Euler didn't give us the table he used to formulate his conjecture, but we may be sure it looked something like the one above. After collecting data, he wrote the following:
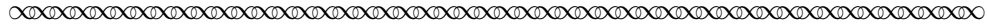
I have also discovered that $2^m + 1$ can be divided if $m = 4p + 1$ or $4p + 2$; while $2^m - 1$ will have the divisor $2m + 1$ if $m = 4p$ or $4p - 1$.

⊗⊗⊗

Task 45 How does Euler's claim match up with yours? Remember that they may mean the same thing, even if they look different initially.

6   More of Euler's Theorems

⊗⊗⊗

I have happened upon many other theorems in this pursuit which are no less elegant, which I believe should be further investigated, because either they cannot be demonstrated themselves, or they follow from propositions which cannot be demonstrated; some which seem important are appended here.
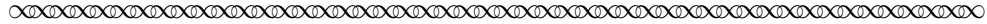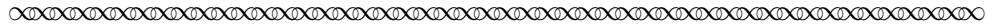
⊗⊗⊗
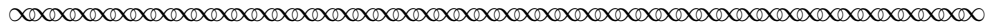
At this point, Euler's paper was almost complete, and he had admitted that he has no more explanations or proofs of his work. For the sake of completeness, we include the rest of the paper here. If you read the next six theorems, you will have read a complete paper of Euler's. (His official catalog lists 866 papers and books — you are now on your way to reading them all!) As an exercise, it may be useful to try to restate each of the theorems using modern notation, including the use of modular arithmetic. Then you might want to try your hand at proving one or two!

⊗⊗⊗

Theorem 1

If n is a prime number, all powers having the exponent $n - 1$ leave either nothing or 1 when divided by n.

Theorem 2

With n still a prime number, every power whose exponent is $n^{m-1}(n - 1)$ leaves either 0 or 1 when divided by n^m.

Theorem 3

Let m, n, p, q etc be distinct prime numbers and let A be the least common multiple of them decreased by unity, think of them $m-1, n-1, p-1, q-1$ etc.; with this done, I say that any power of the exponent A, like a^A, divided by $mnpq$ etc. will leave either 0 or 1, unless a can be divided by one of the numbers m, n, p, q etc.

Theorem 4

With $2n+1$ denoting a prime number, 3^n+1 will be able to be divided by $2n+1$, if either $n = 6p+2$ or $n = 6p+3$; while 3^n-1 will be able to be divided by $2n+1$ if either $n = 6p$ or $n = 6p-1$.

Theorem 5

$3^n + 2^n$ can be divided by $2n+1$ if $n = 12p+3$, $12p+5$, $12p+6$ or $12p+8$, And $3^n - 2^n$ can be divided by $2n+1$ if $n = 12$, $12p+2$, $12p+9$ or $12p+11$.

Theorem 6

Under the same conditions which held for $3^n + 2^n$, $6^n + 1$ can also be divided by $2n+1$; and $6^n - 1$ under those which held for $3^n - 2^n$.
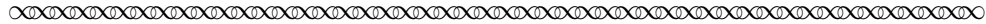
References

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. A complete English translation by Jordan Bell (University of Toronto) is available at `https://scholarlycommons.pacific.edu/euler-works/26/`.

Appendix I: Peering into Euler's Mystery

In Section 2, we marveled at the fact that Euler "mysteriously" found that 641 is a factor of $2^{2^5} + 1$. Now that we understand Euler's Theorem, we can make a good guess as to how Euler was probably able to do this. Since we know that Euler's Theorem is equivalent to Fermat's Little Theorem (which is less complicated to apply in this case), we use the latter theorem in this Appendix to explore this mystery. To streamline the explanation further, we also use the notation of modular arithmetic. Restating Fermat's Little Theorem in that notation, we have:

> **Fermat's Little Theorem**
> For any prime p, and any integer a that is not divisible by p, $a^{p-1} \equiv 1 \pmod{p}$.

The basic idea behind Euler's secret is one that we've seen him use elsewhere in his paper. Namely, it turns out that we can use Fermat's Little Theorem to greatly restrict the possible prime divisors of $2^{2^n} + 1$, and thus make it far easier to find a factor. Let's start by seeing what we can learn about the form of prime divisors of $2^{2^n} + 1$ from Fermat's Little Theorem.

Suppose p is a prime divisor of $2^{2^n} + 1$, or $2^{2^n} + 1 \equiv 0 \pmod{p}$. Rewriting this as the congruence $2^{2^n} \equiv -1 \pmod{p}$ reveals two useful facts. First, that p is odd; and second that $2^{2^{n+1}} \equiv 1 \pmod{p}$.

Task I.1 Let s be the smallest positive integer for which $2^s \equiv 1 \pmod{p}$.

    (a) Prove that s must divide any m for which $2^m \equiv 1 \pmod{p}$.
        (This is straightforward using division with remainder on exponents.)
        Taking $m = 2^{n+1}$ in the useful congruence fact $2^{2^{n+1}} \equiv 1 \pmod{p}$, part (a) of this Task tells us that s divides 2^{n+1}. This means that $s = 2^k$ for some k.

    (b) Prove by contradiction that k cannot be smaller than $n + 1$, and thus $s = 2^{n+1}$. *Hint: Remember both the definition of s and our initial assumption that $2^{2^n} \equiv -1 \pmod{p}$.*

Here's where Fermat's Little Theorem comes in. Since p is an odd prime, we can use Fermat's Little Theorem with $a = 2$ to conclude that $2^{p-1} \equiv 1 \pmod{p}$. Using Task I.1(a) once more (this time with $m = p - 1$), we see that $s = 2^{n+1}$ divides $p - 1$. From this, we conclude that p must be 1 more than a multiple of 2^{n+1}.

Task I.2 (a) What do the preceding arguments imply about the form of any prime factor of $2^{2^5} + 1$?

    (b) Write down the first 10 numbers that have the form you described in part (a). If Euler wanted to see whether $2^{2^5} + 1$ was divisible by any of these, he needed only to check those that are prime. How many of these are divisible be 3 or 5, and so are obviously not prime? How many of the remaining numbers in your list might Euler have had to check?

Observations on a certain theorem of Fermat and on others concerning prime numbers[*]

Leonhard Euler

It is known that the quantity $a^n + 1$ always has divisors whenever n is an odd number or is divisible by an odd number aside from unity.[1] Namely $a^{2m+1} + 1$ can be divided by $a + 1$ and $a^{p(2m+1)} + 1$ by $a^p + 1$, for whatever number is substituted in place of a. But on the other hand, if n is a number which is divisible by no odd number aside from unity, which happens when n is a power of two, no divisor of the number $a^n + 1$ can be assigned.[2] So if there are prime number of this form $a^n + 1$, they must all necessarily be included in the form $a^{2^m} + 1$. But it cannot however be concluded from this that $a^{2^m} + 1$ always exhibits a prime number for any a; for it is clear first that if a is an odd number, this form will have the divisor 2. Then also, even if a denotes an even number, innumerable cases can still be given in which a composite number results. For instance, the formula $a^2 + 1$ can be divided by 5 whenever $a = 5b \pm 3$, and $30^2 + 1$ can be divided by 17, and $50^2 + 1$ by 41. Similarly, $10^4 + 1$ has the divisor 73, $6^8 + 1$ has the divisor 17, and $6^{128} + 1$ is divisible by 257. Yet no case has been found where any divisor of this form $2^{2^m} + 1$ occurs, however far we have checked in the table of prime numbers, which indeed does not extend beyond 100000. For this and perhaps other reasons, Fermat was led to state there to be no doubt that $2^{2^m} + 1$ is always a prime number, and proposed this eminent theorem to Wallis and other English Mathematicians for demonstration. Indeed he admits to not himself have a demonstration of this, but did not however hold it to be any less than completely true. He also praised the great utility of this, by means of which one can easily exhibit a prime number larger than any given number, which without a universal theorem of this type would be very difficult. This is assembled in the penultimate letter in the *Commercium Epistolicum*,

---

[*]Presented to the St. Petersburg Academy on September 26, 1732. Originally published as *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus*, Commentarii academiae scientiarum Petropolitanae **6** (1738), 103–107. E26 in the Eneström index. Translated from the Latin by Jordan Bell, Department of Mathematics, University of Toronto, Toronto, Ontario, Canada. Email: jordan.bell@gmail.com

[1]Translator: If $n = kl$ then $a^n + 1$ is divisible by

$$\frac{a^{kl}}{a^l} = a^{(k-1)l} - a^{(k-2)l} + \ldots + 1.$$

See Chapter II of Hardy and Wright.

[2]Translator: Euler probably means that there is no general form for a divisor.

1

included in the second volume of the *Opera* of Wallis.[3] They are also recorded on p. 115 of the works of Fermat, as follows: "For I have said that numbers made by squaring two and adding unity always lead to prime numbers, namely that $3, 5, 17, 257, 65537$ etc. to infinity are prime, and the truth of this theorem has already been shown by Analysts with no difficulty etc."

The truth of this theorem can be seen, as I have already said, if one takes $1, 2, 3$ and 4 for m; for these yields the numbers $5, 7, 257$ and 65537, which all occur among the prime numbers in the table. But I do not know by what fate it turned out that the number immediately following, $2^{2^5} + 1$, ceases to be a prime number; for I have observed after thinking about this for many days that this number can be divided by 641, which can be seen at once by anyone who cares to check. For it is $2^{2^5} + 1 = 2^{32} + 1 = 4294967297$. From this it can be understood that the theorem fails in this and even in other cases which follow, and hence the problem of finding a prime number greater than a given number still remains unsolved.

I will now examine also the formula $2^n - 1$, which, whenever n is not a prime number, has divisors, and not only $2^n - 1$, but also $a^n - 1$. But if n is a prime number, it might seem that $2^n - 1$ also always gives a prime; this however no one, as far as I know, has dared to profess, and indeed it can easily be refuted. Namely $2^{11} - 1$, i.e. 2047, has the divisors 23 and 89, and $2^{23} - 1$ can be divided by 47. I see also that the Cel. Wolff has not only not mentioned this in the new edition of his *Elem. Matheseos*, where he investigates the perfect numbers and includes 2047 among the primes, but also has 511 or $2^9 - 1$ as a prime, while it is divisible by $2^3 - 1$, i.e. 7. He also gives that $2^{n-1}(2^n - 1)$ is a perfect number whenever $2^n - 1$ is prime; therefore n must also be a prime number. I have found it a worthwhile effort to examine those cases in which $2^n - 1$ is not a prime number while n is. I have also found that $n = 4m - 1$ and $8m - 1$ are prime numbers, then $2^n - 1$ can always be divided by $8m - 1$. Hence the following cases should be excluded: 11, 23, 83, 131, 179, 191, 239 etc., which numbers when substituted for n yield $2^n - 1$ that is a composite number. Neither however can all the remaining prime numbers be successfully put in place of n, but still more must be removed; thus I have observed that $2^{37} - 1$ can be divided by 223, $2^{43} - 1$ by 431, $2^{29} - 1$ by 1103, $2^{73} - 1$ by 439; however it is not in our power to exclude them all. Still, I venture to assert that except for those cases noted, all prime numbers less than 50 and perhaps even 100 yield $2^{n-1}(2^n - 1)$ which is a perfect number, thus 11 perfect numbers arise from the following numbers taken for n, 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47. I have deduced these observations from a not inelegant theorem, whose proof I do not have, but indeed of whose truth I am completely certain. This theorem is: *$a^n - b^n$ can always be divided by $n + 1$, if $n + 1$ is any prime number which divides neither a or b*; I believe this demonstration is more difficult because it is not true unless $n + 1$ is a prime number. From this theorem, it follows at once that $2^n - 1$ can always be divided

---

[3]Translator: See Chapter III, §IV of Weil, *Number theory: an approach through history from Hammurapi to Legendre.*

by $n+1$ if $n+1$ is a prime number, or, since each prime aside from 2 is odd, and as $a = 2$ that case does not happen because of the conditions of the theorem,[4] $2^{2m} - 1$ will always be able to be divided by $2m+1$ if $2m+1$ is a prime number. Hence either $2^m + 1$ or $2^m - 1$ will be able to be divided by $2m+1$.[5] I have also discovered that $2^m + 1$ can be divided if $m = 4p+1$ or $4p+2$; while $2^m - 1$ will have the divisor $2m+1$ if $m = 4p$ or $4p-1$. I have happened upon many other theorems in this pursuit which are no less elegant, which I believe should be further investigated, because either they cannot be demonstrated themselves, or they follow from propositions which cannot be demonstrated; some which seem important are appended here.

Theorem 1

If n is a prime number, all powers having the exponent $n-1$ leave either nothing or 1 when divided by n.

Theorem 2

With n still a prime number, every power whose exponent is $n^{m-1}(n-1)$ leaves either 0 or 1 when divided by n^m.

Theorem 3

Let m, n, p, q etc be distinct prime numbers and let A be the least common multiple of them decreased by unity, think of them $m-1, n-1, p-1, q-1$ etc.; with this done, I say that any power of the exponent A, like a^A, divided by $mnpq$ etc. will leave either 0 or 1, unless a can be divided by one of the numbers m, n, p, q etc.

Theorem 4

With $2n+1$ denoting a prime number, $3^n + 1$ will be able to be divided by $2n+1$, if either $n = 6p+2$ or $n = 6p+3$; while $3^n - 1$ will be able to be divided by $2n+1$ if either $n = 6p$ or $n = 6p-1$.

Theorem 5

$3^n + 2^n$ can be divided by $2n+1$ if $n = 12p+3$, $12p+5$, $12p+6$ or $12p+8$, And $3^n - 2^n$ can be divided by $2n+1$ if $n = 12, 12p+2, 12p+9$ or $12p+11$.

---

[4]Translator: If $n+1 = 2$ then $n+1$ divides a.

[5]Translator: $2^{2m-1} = (2^m + 1)(2^m - 1)$, and since $2m+1$ is prime and divides 2^{2m-1}, it must divide one of the factors.

Theorem 6

Under the same conditions which held for $3^n + 2^n$, $6^n + 1$ can also be divided by $2n + 1$; and $6^n - 1$ under those which held for $3^n - 2^n$.

OBSERVATIONES DE THEO-
REMATE QVODAM FERMATIANO, ALIISQVE
AD NVMEROS PRIMOS SPECTANTIBVS.

AVCTORE
Leonh. Eulero.

NOtum eft hanc quantitatem $a^n + 1$ femper ha-
bere diuifores, quoties n fit numerus impar,
vel per imparem praeter vnitatem diuifibilis.
Namque $a^{2m+1} + 1$ diuidi poteft per $a + 1$ et $a^{p(2m+1)}$
$+ 1$ per $a^p + 1$, quicunque etiam numerus loco a
fubftituatur. Contra vero fi n fuerit eiusmodi nume-
rus, qui per nullum numerum imparem nifi vnitatem
diuidi poffit, id quod euenit, quando n eft dignitas bi-
narii, nullus numeri $a^n + 1$ poteft affignari diuifor.
Quamobrem fi qui funt numeri primi huius formae $a^n + 1$,
ii omnes comprehendantur neceffe eft in hac forma
$a^{2^m} + 1$. Neque tamen ex hoc poteft concludi $a^{2^m} + 1$
femper exhibere numerum primum quicquid fit a; primo
enim perfpicuum eft, fi a fit numerus impar, iftam formam
diuiforem habiturum 2. Deinde quoque, etiamfi a
denotet numerum parem, innumeri tamen dantur ca-
fus, quibus numerus compofitus prodit. Ita haec fal-
tem formula $a^2 + 1$ poteft diuidi per 5, quo-
ties eft $a = 5 b + 3$, et $30^2 + 1$ poteft diuidi per
17, et $50^2 + 1$ per 41. Simili modo $10^4 + 1$ habet
diuiforem 73; $6^8 + 1$ habet diuiforem 17, et 6^{128}
$+ 1$ eft diuifibilis per 257. At huius formae $2^{2^m} + 1$

quan-

quantum ex tabulis numerorum primorum, quae quidem non vltra 100000 extenduntur, nullus detegitur cafus, quo diuifor aliquis locum habeat. Hac forte aliisque rationibus *Fermatius* adductus enunciare non dubitauit $2^{2^m} + 1$ femper effe numerum primum, hocque vt eximium theorema *Wallifio* aliisque Mathematicis Anglis demonftrandum propofuit. Ipfe quidem fatetur fe eius demonftrationem non habere, nihilo tamen minus afferit effe veriffimum. Vtilitatem eius autem hanc potiffimum praedicat, quod eius ope facile fit numerum primum quouis dato maiorem exhibere, id quod fine huiusmodi vniuerfali theoremate foret difficillimum. Leguntur haec in *Wallifii* Commercio Epiftolico Tomo Eius Operum fecundo inferto, epiftola penultima. Extant etiam in ipfius *Fermatii* operibus p. 115. fequentia. "Cum autem numeros a binario quadratice "in fe ductos et vnitate auctos effe femper numeros "primos apud me conftet, et iam dudum Analyftis illius theorematis veritas fuerit fignificata nempe effe "primos 3, 5, 17, 257, 65537, etc. in infinit. nullo "negotio etc.

Veritas iftius theorematis elucet, vt iam dixi, fi pro m ponatur 1, 2, 3 et 4, prodeunt enim hi numeri 5, 17, 257, et 65537, qui omnes inter numeros primos in tabula reperiuntur. Sed nefcio, quo fato eueniat, vt ftatim fequens nempe $2^{2^5} + 1$ ceffet effe numerus primus, obferuaui enim his diebus longe alia agens poffe hunc numerum diuidi per 641. vt cuique tentanti ftatim patebit.

Eft

Est enim $2^{25} + 1 = 2^{32} + 1 = 4294967297$. Ex quo intelligi poteft, theorema hoc etiam in aliis, qui fequuntur, cafibus fallere, et hanc ob rem problema de inueniendo numero primo quouis dato maiore etiam nunc non effe folutum.

Confiderabo nunc etiam formulam $2^n - 1$, quae quoties n non eft numerus primus, habet diuifores: neque tantum $2^n - 1$ fed atiam $a^n - 1$. Sed fi n fit numerus primus, videri poffet etiam $2^n - 1$ femper talem exhibere: hoc tamen affeuerare nemo eft aufus quantum fcio, cum tam facile potuiffet refelli. Namque $2^{11} - 1$ i.e. 2047 diuifores habet 23 et 89 et $2^{23} - 1$ diuidi poteft per 47. Video autem Cel. *Wolfium* non folum hoc in Elem. Mathefeos editione altera non aduertiffe, vbi numeros perfectos inueftigat, atque 2047 inter primos numerat; fed etiam 511 feu $2^9 - 1$ pro tali habet, cum tamen fit diuifibilis per $2^3 - 1$ i. e. 7. Dat autem $2^{n-1}(2^n - 1)$ numerum perfectum, quoties $2^n - 1$ eft primus, debet ergo etiam n effe numerus primus. Operae igitur pretium fore exiftimaui eos notare cafus, quibus $2^n - 1$ non eft numerus primus, quamuis n fit talis. Inueni autem hoc femper fieri, fi fit $n = 4m - 1$, atque $8m - 1$ fuerit numerus primus, tum enim $2^n - 1$ femper poterit diuidi per $8m - 1$. Hinc excludendi funt cafus fequentes, 11, 23, 83, 131, 179, 191, 239, etc. qui nümeri pro n fubftituti reddunt $2^n - 1$ numerum compofitum. Neque tamen reliqui numeri primi omnes loco n pofiti fatisfaciunt, fed plures infuper excipiuntur, fic obferuaui $2^{37} - 1$ diuidi poffe per 223, $2^{43} - 1$ per

Tom. VI.　　　　　O　　　　　431,

431, $2^{29}-1$ per 1103, $2^{73}-1$ per 439, omnes tamen excludere non est in potestate. Attamen asserere audeo praeter hos casus notatos, omnes numeros primos minores quam 50, et forte quam 100, efficere $2^{n-1}(2^{n}-1)$ esse numerum perfectum, sequentibus numeris pro n positis, 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47, vnde 11 proueniunt numeri perfecti. Deduxi has obseruationes ex Theoremate quodam non ineleganti, cuius quidem demonstrationem quoque non habeo, verum tamen de eius veritate sum certissimus. Theorema hoc est, $a^{n}-b^{n}$, semper potest diuidi per $n+1$, si $n+1$ fuerit numerus primus atque a et b non possint per eum diuidi; eo autem difficiliorem puto eius demonstrationem esse, quia non est verum nisi $n+1$ sit numerus primus. Ex hoc statim sequitur $2^{n}-1$ semper diuidi posse per $n+1$, si fuerit $n+1$ numerus primus, seu cum omnis primus sit impar praeter 2, hicque ob conditiones theorematis, quia est $a = 2$, non possit adhiberi, poterit $2^{2m}-1$ semper diuidi per $2m+1$ si $2m+1$ sit numerus primus. Quare etiam vel $2^{m}+1$ vel $2^{m}-1$ diuidi poterit per $2m+1$. Deprehendi autem $2^{m}+1$ posse diuidi, si fuerit $m = 4p+1$ vel $4p+2$, at $2^{m}-1$ habebit diuisorem $2m+1$, si $m = 4p$ vel $4p-1$. Haec persecutus in multa alia incidi theoremata non minus elegantia, quae eo magis aestimanda esse puto, quod vel demonstrari prorsus nequeant, vel ex eiusmodi propositionibus sequantur, quae demonstrari non possunt, primaria igitur hic adiungere visum est.

Theo-

Theorema I. Si fuerit n numerus primus, omnis potentia exponentis $n-1$ per n diuisa vel nihil vel 1 relinquit.

Theorema II. Manente n numero primo, omnis potentia, cuius exponens est $n^{m-1}(n-1)$, diuisa per n^m vel o vel 1 relinquit.

Theorema III. Sint m, n, p, q, etc. numeri primi inaequales, sitque A minimus communis diuiduus eorum vnitate minutorum, puta ipsorum $m-1$, $n-1, p-1, q-1$, etc. his positis dico omnem potentiam exponentis A vt a^A diuisam per $m n p q$ etc. vel o vel 1 relinquere, nisi a diuidi possit per aliquem horum numerorum, m, n, p, q etc.

Theorema IV. Denotante $2n+1$ numerum primum poterit 3^n+1 diuidi per $2n+1$, si sit vel $n=6p+2$ vel $n=6p+3$: at 3^n-1 diuidi poterit per $2n+1$ si sit vel $n=$ vel $6p$ vel $n=6p-1$.

Theorema V. 3^n+2^n potest diuidi per $2n+1$ si sit $n=$ vel $12p+3$, vel $12p+5$, vel $12p+6$, vel $12p+8$. Atque 3^n-2^n potest diuidi per $2n+1$, si sit $n=$ vel $12p$ vel $12p+2$, vel $12p+9$, vel $12p+11$.

Theorema VI. Sub iisdem conditionibus quibus 3^n+2^n poterit etiam 6^n+1 diuidi per $2n+1$; atque 6^n-1 sub iisdem, quibus 3^n-2^n.

Da-

Notes to Instructors

PSP Content: Topics and Goals

This Primary Source Project (PSP) is slightly different in its approach from other projects that use a guided reading approach to primary historical sources. Although it addresses a significant number of topics from a standard Number Theory course, its focus is on making sense of the mathematics in a single source, and the complete text of the source at that! Euler's *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus*[6], has long been one of my favorite in the history of mathematics. Euler's E26 is his first paper in the field of number theory, and is eminently readable. It contains enough detail that it can be followed, but there is enough missing to make it a perfect paper for students to work through. Furthermore, Euler touched on a surprising number of the standard topics in a first number theory course: using "modular arithmetic" (though the modern version of this did not yet exist) to show that some particular forms of numbers must always be composite, and giving introductions to Fermat primes, Mersenne primes, perfect numbers, and Fermat's Little Theorem. By working through Euler's paper, students can make discoveries in the same way many number theorists do, by playing with patterns, making conjectures, and then looking for proofs. As a bonus, students can try their hand at proving some results that Euler believed were true, but that even he couldn't prove when he wrote this paper!

Student Prerequisites

Euler wrote this paper expecting the reader to have a strong (elementary) algebra background, but not to know any number theory. I've used in a lower-division Honors Seminar for first-year students, and indeed it could be used on the first day of class. The type of algebraic thinking Euler expected of his readers, though technically elementary, may be more sophisticated than we can expect of most college students.

Instructors have achieved the most success with this project, I think, by making sure students are comfortable with modular arithmetic and basic number-theoretic reasoning, perhaps at the level of the first three weeks of a first course in the field.

PSP Design and Task Commentary

This PSP consists of 6 main sections and an optional appendix.

- **Sections 1–2**: Introduction and Fermat Primes (1.5 class days)

  After a short introduction, Section 2 explores the first part of Euler's paper, which concerns factors of numbers of the form $a^n + 1$. Tasks 1–5 introduce students to Euler's vocabulary and encourage an inquiry-based approach to exploring some of his ideas. Tasks 6–7 also allow students to examine claims about factors of numbers of the form a^{2m+1} using techniques of elementary algebra, while Task 8 again encourages students to find their own examples both to test and to understand a claim of Euler that is not written as carefully as a similar claim would be using modern standards.

---

[6]English translation: *Observations on a theorem of Fermat and others concerned with prime numbers.* This paper is given designation E26 by standard catalog of Euler's works as prepared by Gustav Eneström.

Task 9 is intended both to "wow" the student and to invite reflection on Euler's rather stupefying discovery that $6^{128} + 1$ is divisible by 257.

Beginning with Task 10, students begin to consider what we now call "Fermat primes," and also have a chance to use Euler's claims to consider the nature of mathematical knowledge.

- **Section 3**: Mersenne primes and perfect numbers (1 class day)

In this section, students discover with Euler the necessary — but not sufficient — condition that n must be prime if $2^n - 1$ is to be prime, and then examine claims of both Euler and Euclid that the primality of $2^n - 1$ implies that the number $2^{n-1}(2^n - 1)$ is perfect.

- **Section 4**: Mersenne and Sophie Germain primes (1 class days)

This section contains interesting ideas concerning Mersenne and Sophie Germain primes. It's fairly short and has no particularly tricky tasks, and thus could even be reasonably assigned as homework (but see the suggestion for a good day of group work in the schedule below).

- **Section 5**: Toward the Euler-Fermat theorem (2 class days)

This is the deepest and most mathematically-intense section of the PSP. In E26, Euler stated, without proof, an early version of the what we now call "Fermat's Little Theorem" or the "Euler-Fermat theorem." Students discover and prove several ideas related to this theorem in this section.

- **Section 6**: More of Euler's Theorems (0–0.5 days)

E26 is unusual in that Euler stated a number of "theorems" that he could not prove at the time. The paper concludes with six of these. They are included here for two reasons: first, after reading them, students will have read every word of one of Euler's papers (in translation). Second, proofs of some of these theorems are within the ability of strong students, who could have the welcome experience of proving something beyond the ability of Euler at the beginning of his number-theoretic work. This section could just be assigned as out-of-class reading.

- **Appendix 1**: One of the most fascinating pieces of E26 is Euler's announcement that 641 is a factor of $F_5 = 2^{2^5} + 1$. How, we may reasonably wonder, could he have discovered this? Although Euler did not explain his methods in this paper, they are lurking behind the scenes. Appendix I guides the reader through a plausible route that Euler may have taken, using results from E26, to turn this discovery into a fairly quick calculation – one any mathematician could do by hand in under half an hour. These methods are very interesting, but since their exploration deviates from Euler's work in a PSP that focuses on that work so directly, they are explored in an optional Appendix.

A few comments on select student tasks follow.

- Tasks 6–7: The solution can be found by "simple" polynomial division, but the algebraic details can be tricky for many students. With a bit of cleverness, the result can also be seen directly using the summation formula for finite geometric sums. If you don't feel strongly that these are skills you want your students to have, they can be given a lot of assistance here, or you can omit these tasks altogether.

- Task 9 (and others): Instructors should spend some time before the start of this PSP deciding how they want students to use computers. At one extreme, all of the "use a computer" tasks in this project could be completed using a smart phone to access `wolframalpha.com`. Alternatively, you may want students to write nice code to solve these questions in a programming language on which your class has focused.

- Task 12 asks students to weigh in on no less than the nature of mathematical truth. Answers to the question could be explored for an entire class period (or more!), if you so chose. Alternatively, you could spend no time on this at all.

- Task 13: Some students will struggle here. When they've struggled enough, suggest that they write down the inequality they want to solve, and take the logarithm of both sides.

- Task 18: This is a nice chance to remind (teach?) students that the ceiling of the base-10 logarithm of an integer gives its number of digits.

- Task 19 is another task that could lead to a lengthy paper or presentation, or could be dispatched swiftly and with little thought. Either choice is fine, and should depend on what the instructor wants to accomplish in their class.

- Task 30 asks for a heuristic approach to an unsolved problem in number theory. As such, it's perhaps not a fair question, and instructors should accept a wide variety of answers. The curious instructor may want to know that an analytic number theorist might reason thus: "The probability that a random integer n is prime is $1/(\log n)$. The probability that $2n + 1$ is prime is (for odd n) independent of the primality of n, and is thus $1/\log(2n + 1)$. The probability that n is Sophie Germain is thus asymptotically $1/(\log(n) \cdot \log(2n + 1))$. The infinite sum

$$\sum_{n=1}^{\infty} \frac{1}{\log(n) \log(2n + 1)}$$

diverges, so we should expect infinitely many Sophie Germain primes."

- Task 35 is arguably a redundant version of Task 12, but it's interesting to see whether students have a different view of this after spending several days with Euler's text.

- Task I.1(b) might be proven as follows: If k cannot be smaller than $n + 1$, then 2^k divides 2^n, yielding $2^{2^n} \equiv 1$, but this can't be true since $2^{2^n} \equiv -1$ by hypothesis, and p is odd. So $s = 2^{n+1}$.

Suggestions for Classroom Implementation

I would suggest giving this project to students after they have learned modular arithmetic, and probably after an initial lesson on divisibility, but before using a textbook's approach to Mersenne primes, Fermat primes, perfect numbers, or Fermat's Little Theorem.

The PSP includes several open-ended discussion questions, and lends itself well to group work. I suggest assigning these questions to groups of three students (or letting students choose their own, as your classroom culture warrants). The schedule given below is based on 50-minute class periods. Time estimates below assume that students will have as homework each night their uncompleted tasks, and may be more aggressive than is necessary. Some instructors who have used the complete PSP in their classrooms have reported doing so over eight days. One instructor has also used this PSP as a replacement for a midterm exam, with students completing the entire PSP outside of class.

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

The following schedule allows full implementation of this project in 5–6 class days.

- **Day 0:** Give a brief (5-minute) introduction to the project, and tell students explicitly that we'll be spending class time on this project for the next few days, to help them get a strong understanding of some concepts which have been tricky for past students to learn. Assign reading of Section 1 (Introduction) and Section 2 (Fermat Primes), Tasks 1–5 as homework.

- **Day 1:** Start with a short class discussion of Tasks 1–5. Then, in groups, students work through Section 2 with the goal of finishing Tasks 6–9. Some fast groups may finish this early, and can be encouraged to keep solving problems together in class with the goal of reducing their homework.

  Homework: Any unfinished tasks through the end of Section 2 (Task 19). However, if students are not particularly strong on mathematical induction, I suggest not assigning parts Tasks 16 and 17 as homework. After trying Task 15 (the easiest induction problem) as homework, students can discuss their proofs together in class, and work together on Tasks 16 and 17. Also see Task 12 note, below.

- **Day 2:** Depending on instructor preference, some time could be spent in groups or as a whole class discussing Task 12, and the proofs of Tasks 16–17. Most of the day is spent on Section 3 (Perfect Numbers), with students completing Tasks 18–23(a), and then starting work on the rest of the section.

  Homework: Task 23(b), and any unfinished tasks through Task 27.

- **Day 3:** Start Section 4 (Mersenne and Sophie Germain Primes), and work in groups on Tasks 28–30.

  Homework: Finish Section 4 (there's only one more task). Start Section 5 (Towards the Euler-Fermat Theorem), completing Tasks 32 and 33.

- **Day 4:** Students work in groups to complete Tasks 34–37 in Section 5. Tasks 38 and 39 can be assigned at the discretion of the instructor, and are probably best for especially strong students / classes.

  Homework: Optional homework described above, or time to catch up.

- **Day 5:** Students work in groups to complete Section 5. **This may take two class days**, but I argue this it's worth the time; the students will be engaged in good number-theoretic thinking the whole time. Section 6 (More of Euler's Theorem) should also be assigned for reading to bring the project to closure.

- **Beyond Day 5:** At the instructor's discretion, time could be spent on the optional Appendix – it could even serve as a reward for finishing this project.

Possible Modifications of the PSP

It would be easy to extend this project by asking students to explore the theorems in Section 6 in the same way they explored the theorems Euler described earlier in the paper. Another option is to note

that after Section 2, the sections are quite independent, and any of them could be omitted to save time without materially compromising the goals of the project.

LaTeX code of this entire PSP is available from the author by request. The PSP itself can also be modified by instructors as desired to better suit their goals for the course.

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 a course on Number Theory. The PSP author name of each is given (together with the number of days required for full implementation). 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 Flagg (3–4 days)
- 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

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