Primes, Divisibility, and Factoring

Dominic Klyve
Department of Mathematics
Central Washington University
Ellensburg WA
Dominic.Klyve@cwu.edu

February 2, 2017

In 1732, Leonhard Euler 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 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, filled with powerful new insights into the nature of integers and primes, to the rest of the academy. 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 finishing reading the paper, you will have the chance to prove several theorems which stumped even Euler.

1 Fermat Primes

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

> 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 makes 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.

(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?

(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.)

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

(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 $3^n + 1$?

(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.

[1] All translations, unless otherwise noted, are taken from the English translation of the original Latin by Jordan Bell, available at http://eulerarchive.maa.org/pages/E026.html

Euler himself makes a claim about divisors of $a^n + 1$ in the second sentence of the paper. He claims

> 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 for $a = 2$ and $a = 3$ in exercises 3 and 4 above. We would, however, like to establish this claim for all values of a.

(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.)

(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 Question (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.

(8) What does Euler seem to be claiming about numbers of the form $a^{2^n} + 1$? Is 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 gives 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 things about this to Euler's contemporaries – and to many moden readers – is the ease with which Euler works 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.

(9) Use a computer or a powerful calculator to find $6^{128} + 1$, and then check whether it is divisible by 257. How do you think Euler could have discovered this fact, given that he lived long before computers and calculators?

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

> 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.

(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.

(11) It seems that when Euler checked if a number was prime, he uses 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 states 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 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.

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."

(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?

(13) Fermat claims 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.

(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 Eulers 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 the following exercises, you will show that $2^{2^m} + 1$ is never divisible by $3, 5$, or 7.

(15) If you have learned mathematical induction, use an induction argument to show that for $m > 0, 2^{2^m} + 1 \equiv 2 \pmod 3$.

(16) If you have learned mathematical induction, use an induction argument to show that for $m > 1, 2^{2^m} + 1$ is never divisible by 5.

(17) Finally, try 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 reduces the number of factors of these special numbers he would need 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 of F_6. How hard would this be?

(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? Try this, and report what you find.

(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, doesn't discuss his methods in this paper, nor does he pursue these questions about Fermat numbers. Instead, he quickly shifts his focus to another kind of prime number.

2 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. 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 Leibniz in 1716. Over the next decades, Wolff wrote hundreds of essays about everything from philosophy, physics to farming to theology.

Euler had first come into contact with Christian Wolff a few years earlier when he stopped to visit him in Marburg while Euler was moving 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 digresses 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.

> 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.

(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 $m = mk$ of two natural numbers m and k both greater than 1.)

(21) Euler then points 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.

(22) Find the next perfect number after 6.

(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. 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 has 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.

(24) What does 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.

(25) Euclid is 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?

(26) What does Euclid mean by "the last"?

(27) Write Euclid's proposition in modern symbolic notation.
How does it compare to Euler's final statement above?

3 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, a seventeenth-century Catholic priest who wrote about numbers of this form. At the same time that Euler wrote his paper, he seems to have been unaware of Mersenne's work, and he makes no mention of Mersenne.

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 Exercise (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 starts 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.

(28) Look at Euler's claim that $2^{4m-1} - 1$ is divisible by $8m - 1$ in certain cases.
Check whether $2^{4m-1} - 1$ is divisible by $8m - 1$ when $m = 1, 2$, and 3.
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 is 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 is 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[2] used these primes (and others) when she tried to prove Fermat's Last Theorem (yes – named for the same Fermat!).

(29) In the previous excerpt, Euler listed seven primes p that he claimed are Sophie Germain primes. Verify that he is correct. (Use a computer or table of primes?) 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. See if you can find a longer chain of such primes. (At the time this project was written, the longest known such chain had 17 primes – can you do better?)

(30) Do you think there are infinitely many Sophie Germain primes?
What evidence or heuristic reasoning can you give for this?

[2] Sophie Germain's story is fascinating – check out *Prime Mystery: The Life and Mathematics of Sophie Germain* by Dora E. Musielak (AuthorHouse Book, 2015) to learn more!

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.[3] Euler listed some of these (the Sophie Germain primes of form $2^{4m-1} - 1$) 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.

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 Gottfried 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.

(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

Remember: You type in things like "Is $2^{13} - 1$ prime?" at `www.wolframalpha.com`.

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.

[3] 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 is able to immediately rule out some cases.

4 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 will develop over the next decades. Let's first make sure we understand what it 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.

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

(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?

(34) Now choose another value of n (larger than 4) which 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.

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

(36) At the end of the excerpt, Euler says "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 it 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.

(37) Prove Euler's theorem when $n = 2$.

(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:

Question (38) continued.

(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 exercise.

(c) For the integers $a = 1, 2, 3, 4$ make a list of the remainders of a^4 divided by 5. (Write these calculations in terms of congruencies mod 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's really going on in Euler's mind. If you're feeling brave, consider trying the next (optional) problem:

(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 is usually written as follows:

Theorem. *For any prime p, and any integer a which is not divisible by p, we have*

$$a^{p-1} \equiv 1 \pmod{p}.$$

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 claim is equivalent to Fermat's little theorem.

(40) By choosing appropriate values of p and b, prove that Euler's claim implies Fermat's little theorem.

(41) Now prove that Fermat's little theorem implies Euler's claim.

(42) Think about what you have done in questions 40 and 41 above.
Have you proven that Euler's claim is true? Explain.

Euler 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 generlization of it (now called the Euler-Fermat theorem), in one of almost a hundred papers he would publish in number theory[4]. Despite his ability to prove it in 1732, Euler was so sure that it was true that he started to apply it to derive other statements. The first of these applications was the next part claim in his 1732 paper. (Note in the following that when Euler writes "this theorem", he is referring to what we have been calling "Euler's Theorem".)

> 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 $2m+1$.

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.

(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).

[4] 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.

At this point, Euler has claimed that when $2m+1$ is prime, either 2^m-1 or 2^m+1 is prime. This isn't fully satisfying, though – we might further ask if there is a way to determine when it is that 2^m-1 is divisible by $2m+1$, and when it is that 2^m+1 that's divisible by $2m+1$? 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).

(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 doesn'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 $4p-1$.

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

5 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.

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

[1] Musielak, Dora E, Prime Mystery: The Life and Mathematics of Sophie Germain (2015). AuthorHouse Books, 2015.