Modern Number Theory by

Fermat and Euler

Long Dang

MATH464WI

Date: 05/12/2023

Word Count: 4645

Pierre de Fermat once said, “Perhaps, posterity will thank me for having shown that the ancients did not know everything.” [10] In the beginning of human civilization around 4,000 BC in Sumeria, people needed a solution for organizing and keeping track of livestock, crops and artisan goods; thus, numbers and counting were invented. However, Sumerian counting represented as a token. For example, if a man has five chickens, he was given five tokens. Roughly 1,000 years later, around 3,000 BC, the Egyptians, transformed the number one from a unit of counting things to a unit of measuring things. Then came Ancient Greece, during which time, there was a revolution in the world of numbers where people like Pythagoras, Archimedes, Diophantus and Euclid, made significant contributions. [7]

In the modern number theory, around 17th century until now, probably one of mathematics biggest amateurs is mathematician Pierre de Fermat (1601 – 1665). Sometimes he would come up with the most groundbreaking and incredible mathematical theorems. Although mathematics was something he liked to do in his free time as, he was actually a lawyer. However, he is considered the founder of modern number theory. Some examples:

1. In 1640, Fermat stated what is known as Fermat’s little theorem.
2. Method of factoring by the difference of two squares.
3. In 1638, Fermat claimed that every whole number can be expressed as the sum of four or fewer squares; however, he asserted to have a proof but did not share it.
4. Fermat’s last theorem or Fermat’s great theorem, there are no natural numbers, n, greater than 2, such that $x^n + y^n = z^n$. [9]

Fermat is famous for his Fermat's numbers with $f(n) = 2^{2^n} + 1$, where he found that the first five such numbers were prime, so he conjectured that every such number was a prime number. Unfortunately, this is false if $n = 5$ so that $2^{32} + 1$ is not a prime number. In fact, every number checked beyond $2^{16} + 1$ is not prime. So now, it's conjectured that the first five numbers was the only prime Fermat's numbers. One application about Fermat's numbers is that no two Fermat's numbers will ever share a common factor, so you can generate a very large prime number by just calculating a Fermat's number and factoring it. Then Fermat's numbers help to show there are just many prime numbers as there are natural numbers.

Our discussion will be on the method of factoring by the difference of two squares.

The first foundation stones towards the creation of modern-day factoring were laid in ancient Mesopotamia, roughly around 5,000 years ago [12]. However, not until the Greek mathematicians was it applied to the case of integers [4]. Later, the ideas went on to rational, irrational, and real numbers; furthermore, methods of factoring expanded to polynomial factorization with various applications, such as coding theory and cryptography where factorization is part of the base from which systems are built or broken. Another application is when modeling phenomena with polynomials, data scientists seek to determine when the polynomial evaluates to zero, hence one of the tools is factoring.

There are three types of methods of factoring. GCF (Greatest Common Factor), Trinomial Factoring and factoring a Difference of Squares [6]. The GCF was found during the process of the Euclidean algorithm, described by the mathematician Euclid in Euclid's *Elements* [2], considered one of the most influential books in the history of mathematics. The ideas of GCF come from finding the GCD (greatest common divisor) of two numbers. The general form of trinomial factoring is polynomial factoring; it was first introduced in public in 1793 by Theodor Von Schuber (1758 – 1825). In 1882, Leopold Kronecker (1823 – 1891) extended it into multivariate polynomials and it was applied in the first computer algebra system in 1965 [4].

We will first examine Fermat's method of factoring by the difference of two squares in 1643. This is a paragraph translated in the History of The Theory of Numbers by Leonard Eugene Dickson, volume 1, chapter 14, in 1952. [2, p. 357] Comments in square brackets are mine.

Methods of factoring

Factoring by method of difference of two squares.

Fermat described his method [in about 1643] as follows:

"An odd number not a square can be expressed as the difference of two squares in as many ways as it is the product of two factors, and if the squares are relatively prime the factors are. But if the squares have a common divisor *d*, the given number is divisible by *d* and the factors by $\sqrt{d}$.

[For instance, 45 is an odd number not a square, $45 = 3 \cdot 15 = 9 \cdot 5$ a product of two factors in two ways, and $45 = 7^2 - 2^2 = 9^2 - 6^2$. Notice that 7^2 and 2^2 are relatively prime as are the factors $9 = 7 + 2$ and $5 = 7 - 2$, while 9^2 and 6^2 have the common divisor 9, 45 is divisible by 9 and the factors $3 = 9 - 6$ and $15 = 9 + 6$ are divisible by $\sqrt{9} = 3$.]

[Example] Given a number *n,* for example *2027651281*, to find if it be prime or composite and the factors in the latter [composite] case. Extract the square root of *n.* I get *r* =

45029, with the remainder *40440* $[45029^2 + 40440 = 2027610841 + 40440 = 2027651281 = n]$. Subtracting the latter $[40440]$ from *2r + 1*, I get *49619*, which is not a square in view of the ending *19*.

[If n is a natural number of two digits or more, then n must end in one of these 22 pair of digits: $00,01,04,09,16,21,24,25,29,36,41,44,49,56,61,64,69,76,81,84,89,96$. So, if n does not end in one of these pairs, it is not a perfect square. See [1].]

Hence I add *90061 = 2 + 2r + 1* to it. Since the sum *139680* is not a square, as seen by the final digits, I again add to it the same number increased by 2, i.e., *90063*, and I can continue until the sum becomes a square. This does not happen until we reach *1040400,* the square of *1020*. For by an inspection of the sums mentioned it is easy to say that the final one is the only square (by their endings except for *499944*).

[The numbers in the right column below are not squares, except for the last number. We see this by looking at their last two digits, except for 499944 which we show is not a square by factoring it as $2^2 \cdot 3 \cdot 37 \cdot 563$. Notice there are 11 additions.

	49619
49,619 + 90,061	= 139,680.
139,680 + 90,063	= 229,743.
229,743 + 90,065	= 319,808
319,808 + 90,067	= 409,875.
409,875 + 90,069	= 499,944.
499,944 + 90,071	= 590,015.
590,015 + 90,073	= 680,088.
680,088 + 90,075	= 770,163.
770,163 + 90,077	= 860,240.
860,240 + 90,079	= 950,319.
950,319 + 90,081	= 1,040,400 = 1020^2.

Not squares because of the last two digits.

.]

To find the factors of *n* [= 2027651281], I subtract the first number added, *90061*, from the last, *90081* [= 20]. To half the difference [10] add *2.* There results *12.* The sum of *12* and the root *r* [= 45029] is *45041*. Adding and subtracting the root *1020* of the final sum *1040400*, we get *46061* [= 45041 + 1020] and *44021* [= 45041 − 1020], which are the two numbers nearest to *r* whose product is *n*

$$[2027651281 = 46061 \cdot 44021 = (45041 + 1020) \cdot (45041 - 1020) = 45041^2 - 1020^2.]$$

They are the only factors since [in this case] they are primes. Instead of *11* additions, the ordinary method of factoring would require the division of all the numbers from *7* to *44021.”*

. . .

G. Wertheim expressed in general form Fermat's method [in about 1896] to factor an odd number *m* [here his *m* is a product of two primes] [2, p. 358].

Let a^2 be the largest square < *m* and set $m = a^2 + t$ [where *t* is the remainder].

[Observe $m = a^2 + t < (a+1)^2 = a^2 + 2a + 1$.]

[Case 1] If $p = 2a + 1 - t$ is a square (k^2), we eliminate *t* [meaning since $2a + 1 - t = k^2$, replace $t = 2a + 1 - k^2$ in *m*]

and get $m = (a + 1 + k) \times (a + 1 - k)$.

[Because $m = a^2 + t = a^2 + (2a + 1 - k^2) = (a+1)^2 - k^2 = (a + 1 + k) \cdot (a + 1 - k)$.]

[Case 2] If p is not a square, add to p [$= 2a + 1 - t$] enough terms of the arithmetic progression $2a + 3, 2a + 5, \ldots$ to give a square: [This is always possible by a previous result.]

$$p + (2a + 3) + \cdots + (2a + 2k - 1) = s^2.$$

Then $2ak + k^2 - t = s^2$ and $m = (a + k)^2 - s^2$.

[Observe $\quad s^2 = p + (2a + 3) + (2a + 5) + \cdots + (2a + 2k - 1)$

$$= 2a + 1 - t + (2a + 1 + 2) + (2a + 1 + 4) + \cdots + (2a + 1 + 2(k-1))$$

$$= -t + k(2a + 1) + 2 + 4 + \cdots + 2(k - 1)$$

$$= -t + k(2a+1) + 2(1+2+\cdots+k-1)$$

$$= -t + k(2a+1) + 2\cdot\frac{(k-1)k}{2}$$

$$= -t + k(2a+1) + (k-1)k$$

$$= -t + k(2a+k)$$

$$= -t + 2ak + k^2.$$

Thus

$$(a+k)^2 - s^2$$

$$= (a+k)^2 - (-t + 2ak + k^2)$$

$$= a^2 + 2ak + k^2 + t - 2ak - k^2$$

$$= a^2 + t$$

$$= m.]$$

The method is the more rapid the smaller the difference between the two factors.

Regardless of Fermat's genius, number theory still was relatively neglected in the last decades of the 17th century, and he dreamed it would become more popular. Credit for introducing number theory into the mainstream, and finally realizing Fermat's dream, is due to the 18th century's greatest mathematician, perhaps one of the greatest mathematicians of all time, Leonhard Euler (1707 – 1783), a Swiss. He was the most prolific mathematician ever and influential. He made significant discoveries in fields such as infinitesimal calculus and graph theory. So, when he turned his attention to number theory, the topic could no longer be ignored.

However, it was Christian Goldbach (1690 – 1764), a number theory enthusiast, inspired by Fermat's work, who caught Euler's attention by the question, "Is Fermat's observation known to you, that all number $2^{2^n}+1$ are primes?" Euler would settle this question by proving $2^{2^5}+1$ is not prime.

We'll discuss Euler's paper on numbers which are the sum of two squares, originally published as *De numeris, qui sunt aggregata duorum quadratorum,* Novi Commentarii cademiae scientiarum Petropolitanae 4 (1758), pp. 3-40. Translated from the Latin by Paul R. Bialek, Department of Mathematics, Trinity International University, Deerfield, Illinois. Comments in square brackets are mine. [8]

On numbers which are the sum of two squares

Leonhard Euler

3. Because each square number is either even, in which case it is divisible by 4 and contained in the form $4a$, or odd, in which case it is contained in the form $8b + 1$, each number formed from two squares will be either

first, a sum of two squares and will be of the form $4a + 4b$, and will therefore be divisible by 4, or

second, a sum of two squares, one odd and one even, and therefore of the form $4a + 8b + 1$, or, really, will be contained in the form $4a + 1$: it will exceed a multiple of four by one, or

third, a sum of two odd squares and will thus be of the form $8a + 1 + 8b + 1$, or, really, will be contained in the form $8a + 2$. Namely, this will be an unevenly even number [Euler's term for even numbers which are not divisible by four.] and will exceed a multiple of eight by two.

Therefore because all odd numbers either exceed a multiple of four by one and are of the form $4n + 1$ or are one less than a multiple of four and are of the form $4n - 1$, it is evident [by the "second" case above] that no odd numbers of the latter form $4n - 1$ are sums of two squares, and thus numbers of this form $4n - 1$ are excluded from the series of numbers which are sums of two squares.

Then, because all unevenly even numbers [not divisible by 4] either exceed a multiple of eight by two so that they are $8n + 2$ or are two less than a multiple of eight so that they are $8n - 2$, it is evident [by the "third" case above] that no [even] numbers of the latter form are sums of two squares, and thus numbers of this form $8n - 2$ are excluded from the series of numbers which are sums of two squares.

Nevertheless, it is still to be properly observed that not all numbers contained in this form $4n + 1$ nor in this form $8n + 2$ are sums of two squares. And so, for example, the numbers of the former form which are excluded are $21, 33, 57, 69, 77, 93, 105, 129$, etc. and certainly of the latter form are those numbers $42, 66, 114, 138, 154$, etc. I will investigate their rule in turn.

4. Nevertheless, still, numbers which are sums of two squares are so connected by a tie between themselves in a certain way that from one number of this kind, infinitely many others of the same nature can be formed. Because by it this will be more easily observed, I will add the following lemmas which are certainly known well enough by all.

[Lemma]

I. If a number p is a sum of two squares, then the numbers $4p, 9p, 16p$ and, in general, *nnp* will be the sums of two squares.

[Proof]

Certainly, because $p = aa + bb$, we will have $4p = 4aa + 4bb$, $9p = 9aa + 9bb$,$16p = 16aa + 16bb$ and $nnp = nnaa + nnbb$, which are similarly sums of two squares.

[End of proof]

[Lemma]

II. If a number p is a sum of two squares, then so will be $2p$ and, in general, $2nnp$ will be a sum of two squares.

[Proof]

Let $p = aa + bb$; we will have $2p = 2aa + 2bb$. But $2aa + 2bb = (a + b)^2 + (a - b)^2$, from which we will have $2p = (a + b)^2 + (a - b)^2$, and therefore also the sum of two squares. From this, moreover, we will have $2nnp = nn(a + b)^2 + nn(a - b)^2$.

[End of proof]

[Lemma]

III. If the even number $2p$ is a sum of two squares, then half of it, p, will also be a sum of two squares.

[Proof]

Let $2p = aa + bb$; the numbers a and b will both be even or [both be] odd. From this, in either case, both $\frac{a+b}{2}$ or $\frac{a-b}{2}$ will be integers. Certainly $aa + bb = 2(\frac{a+b}{2})^2 + 2(\frac{a-b}{2})^2$, which, by substituting values, is $p = (\frac{a+b}{2})^2 + (\frac{a-b}{2})^2$.

[End of proof]

From this, therefore, all even numbers which are sums of two squares, by continual halving, are finally returned to odd numbers of the same nature. Therefore, again, if only odd numbers which are sums of two squares are known, all such even numbers will be derived from these as well, by continual duplication.

Next it is proper to record the following theorem, by which the nature of the numbers which are sums of two squares is not usually shown.

Theorem

If p and q are two numbers, each of which is the sum of two squares, then their product pq will also be the sum of two squares.

Proof

Let $p = aa + bb$ and $q = cc + dd$. We will have $pq = (aa + bb)(cc + dd) = aacc + aadd + bbcc + bbdd$, which expression can be represented in this way so that $pq = aacc + 2abcd + bbdd + aadd - 2abcd + bbcc$ and for that reason $pq = (ac + bd)^2 + (ad - bc)^2$, from which the product pq will be a sum of two squares. Q.E.D [quod erat demonstrandum, “what was to be demonstrated.”]

From this proposition it follows that when however many numbers which individually are sums of two squares are multiplied together, the product will always be a sum of two squares. And from the given general form, it is evident that the product of two such numbers doubled just recently [possibly referring to the proof of Section 4, Lemma II above] can be partitioned into two squares: so, if $p = aa + bb$ and $q = cc + dd$, then $pq = (ac + bd)^2 + (ad - bc)^2$ and $pq = (ac - bd)^2 + (ad + bc)^2$, which will be a different formula, unless either $a = b$ or $c = d$. Thus [for example], since $5 = 4 + 1$ and $13 = 4 + 9$, the product $5 \cdot 13$ will be the sum of two squares in two ways, namely $65 = (1 \cdot 3 + 2 \cdot 2)^2 + (2 \cdot 3 - 1 \cdot 2)^2 = 49 + 16$, and $65 = (2 \cdot 2 - 1 \cdot 3)^2 + (2 \cdot 3 + 1 \cdot 2)^2 = 1 + 64$. Also, if a product of many numbers is considered, the terms of which are sums of two squares, it can be partitioned in many ways into the sum of two squares. So [for example] if the number $1105 = 5 \cdot 13 \cdot 17$ is put forward, its partitions into two squares will be these: $1105 = 33^2 + 4^2 = 32^2 + 9^2 = 31^2 + 12^2 = 24^2 + 23^2$, namely, the four partitions here.

We now will explicate some later theorems of Euler.

Proposition III

19. If the sum of two squares prime between themselves [meaning “relatively prime” to each other] $aa + bb$ is divisible by a prime number p, a sum of two other squares $cc + dd$ can always be generated which is divisible by that same number p so that the sum $cc + dd$ is not greater than $\frac{1}{2}pp$.

Proof

Let the sum of two squares prime between themselves $aa + bb$ be divisible by the number p, and let a and b be numbers of any size. Therefore, because neither a nor b is divisible by p, the numbers a and b can be expressed as $a = mp \pm c$ and $b = np \pm d$, where one may select m and n [large enough] so that c and d do not exceed $\frac{1}{2}p$. Therefore $aa + bb = mmpp \pm 2mcp + cc + nnpp \pm 2ndp + dd$. Because both this whole expression is divisible by p, by hypothesis, and a part of it, $mmpp \pm 2mcp + nnpp \pm 2ndp$ by itself has p as a divisor, it is necessary that the other part $cc + dd$, which is a sum of two squares, is similarly divisible by p. But because the roots c and d do not exceed $\frac{1}{2}p$, neither of the formulas [terms] in the sum of squares $cc + dd$ will exceed the square pp, and therefore a sum of two squares $cc + dd$ can be produced which is not greater than $\frac{1}{2}pp$ [since $c^2 + d^2 < (\frac{1}{2}p)^2 + (\frac{1}{2}p)^2 = \frac{1}{4}p^2 + \frac{1}{4}p^2 = \frac{1}{2}p^2$], but is nonetheless divisible by p. Q.E.D

Proposition IV

22. The sum of two squares prime between themselves [meaning “relatively prime to each other] cannot be divided by any number which itself is not a sum of two squares.

Proof

[Contradiction]

Concerning what is to be proved, let us suppose that the sum of two squares prime between themselves $aa + bb$ is divisible by the number p, which is not a sum of two squares. Therefore [by Proposition III], another sum of two squares prime between themselves can be generated, $cc + dd$, which is not greater than $\frac{1}{2}pp$ and is divisible by p.

Therefore, let $cc + dd = pq$. Since p is not a sum of two squares, either the number q itself will not be such a sum or will have at least one factor r which is not the sum of two squares. [by Proposition II]

Indeed, because $pq < \frac{1}{2}pp$, we have $q < \frac{1}{2}p$ and, furthermore [since r is a factor of q], $r < \frac{1}{2}p$. Therefore because $cc + dd$ is also divisible by $r < \frac{1}{2}p$, by the preceding proposition, a sum of two squares $ee + ff$ can be generated which is divisible by the same number r and does not exceed $\frac{1}{2}rr$ or, furthermore, $\frac{1}{8}pp$ [$r < \frac{1}{2}p$ implies $\frac{1}{2}r^2 < \frac{1}{2}(\frac{1}{2}p)^2 = \frac{1}{8}p^2$]. And since r is not a sum of two squares, proceeding continuously in a similar way, one reaches smaller sums of two squares which are divisible by a number that is not a sum of two squares. On account of this, because there is no sum of two squares prime between themselves among the smallest numbers and divisible by a number that is not the sum of two squares [which is our contradiction] neither among the greatest numbers will there be such sums of two squares which are divisible by numbers that are not themselves sums of two squares. Q.E.D.

• • •

Scholium

28. All prime numbers which are sums of two squares, except 2, form this series: $5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149$, etc. Not only are these contained in the form $4n + 1$, but also, however far the series is continued, we find that every prime number of the form $4n + 1$ occurs. From this, we can conclude by [logical] induction [not mathematical induction] that it is likely enough that there is no prime number of the form $4n + 1$ which is not also a sum of two squares. Nevertheless, [logical] induction, however extensive, cannot fulfill the role of proof. Even if no one doubts the truth of the statement that all prime numbers of the form $4n + 1$ are sums of two squares, until now mathematics could not add this to its established truths.

Even Fermat declared that he had found a proof, but because he did not publish it anywhere, we properly extend confidence toward the assertion of this most profound man, and we believe that property of the numbers, but this recognition of ours rests on pure faith without knowledge. Although I labored much in vain on a proof to be discarded, nevertheless I have discovered another argument to be given for this truth, which, even it if it is not fully rigorous, still appears to be equivalent to [logical] induction connected with nearly rigorous proof.

Proposition V

[29.] Every prime number which exceeds a multiple of four by one is a sum of two squares.

Attempt at a proof

The prime numbers which this discussion concerns are contained in the form $4n + 1$. Now if the number $4n + 1$ is prime, I showed [in an earlier paper] that the form $a^{4n} - b^{4n}$ is always divisible by it, regardless of what numbers are substituted for a and b, provided that neither is divisible by $4n + 1$. Because $a^{4n} - b^{4n} = (a^{2n} - b^{2n})(a^{2n} + b^{2n})$, it is necessary that one of the factors, either $a^{2n} - b^{2n}$ or $a^{2n} + b^{2n}$, be divisible by the prime number $4n + 1$. Accordingly, as a and b assume some values or others, in some cases the formula $a^{2n} - b^{2n}$ and in other cases the formula $a^{2n} + b^{2n}$ will divisible by $4n + 1$. From this, one may assume, if indeed I am not yet able to overcome this with a solid proof, that such numbers can always be assigned for a and b so that the formula $a^{2n} - b^{2n}$ is not divisible by $4n + 1$; therefore, in these cases, the other formula $a^{2n} + b^{2n}$ must necessarily be divisible by $4n + 1$.

…

Let $a^n = p$ and $b^n = q$. The sum of two squares $pp + qq$ obtained is divisible by $4n + 1$ even though neither square pp nor qq individually has $4n + 1$ as a divisor. And therefore, even if perhaps pp and qq have a common divisor mm, so that $pp + qq = mm(rr + ss)$, because the common factor mm does not have $4n + 1$ as a divisor, it is necessary that the sum of two squares prime between themselves $rr + ss$ has $4n + 1$ as a divisor. Consequently, because such a sum of two squares does not allow other divisors, it is necessary that the prime number $4n + 1$ be a sum of two squares.

[End of proof attempt]

Scholium

31. These cases of a for which the formula $a^{2n} - 1$ is divisible by the prime number $4n + 1$ can be easily determined. **First**, for instance, if $a = pp$, then the formula $a^{2n} - 1 = p^{4n} - 1$ is always divisible by $4n + 1$, provided that p does not equal $4n + 1$ or a multiple of it. **Next**, if $a = pp \pm (4n + 1)q$, the formula $a^{2n} - 1$ also has $4n + 1$ as a divisor, for $a^{2n} = (pp \pm (4n + 1)q)^{2n}$ can be broken up into a series of terms, of which the first is p^{4n}, and

each of the subsequent terms is divisible by $4n+1$. From this, it is evident that the appropriate values for a are all the residues which remain after squares p^2 are divided by $4n+1$. However, whether r or $4n+1+r$ or $(4n+1)q+r$ is substituted for a, these same residues occur, from which all possible residues are obtained if p is set equal to successive numbers $1, 2, 3, 4, 5$, up to $4n$. But setting p equal to the value $4n$ yields the same residue as the value 1, and in a similar way, the values 2 and $4n-1$ give the same residue; so do 3 and $4n-2$; so do 4 and $4n-3$, etc.

Thus, whenever two residues arising form the numbers $1, 2, 3$, up to $4n$ for the roots of squares are equal, the number of different such resulting residues will be $2n$, and therefore this many numbers will be generated less than $4n+1$, numbers which cannot be residues arising from division of square numbers by $4n+1$. And these numbers substituted for a always produce a number $a^{2n}-1$ which is not divisible by $4n+1$. **Indeed, this similarly cannot be proven.** And yet, because in making the attempt, however many numbers are explored in this way, not a single case will occur which contradicts this rule, its truth should be acknowledged. I will attach several examples in which these things are observed more clearly.

First, let $4n+1=5$: cases for which the formula a^2-1 is divisible by 5 [$a^2-1=5k$, so $a^2=5k+1$] will be obtained if for a is a substituted the residues arising from division of squares by 5; these residues are $1, 4$ [because the only way $a^2=5k+1$ is when $a=5j+1$ or $a=5j+4$]. But if a is set equal to either 2 or 3, the formula a^2-1 will not be divisible by 5; in these cases therefore the formula a^2+1 will have 5 as a divisor.

Now let $4n+1=13$, namely, let $n=3$. The residues which are left after the division of square numbers by 13 are $1, 4, 9, 3, 12, 10$. Consequently, if any of the remaining numbers

$2, 5, 6, 7, 8, 11$, are substituted for a, then not the formula $a^6 - 1$, but $a^6 + 1$ will be divisible by 13.

Next, if $4n + 1 = 17$, that is, if $n = 4$, because the residues of squares divided by 17 are $1, 4, 9, 16, 8, 2, 15, 13$, if any of the remaining numbers $3, 5, 6, 7, 10, 11, 12, 14$ is set equal to a, then the formula $a^8 - 1$ will not be divisible by 17, but $a^8 + 1$ will be.

Therefore, because this principle is observed continually, this proof via [logical] induction will be judged almost complete. Hence, this proposition seems so confirmed that one may not voice much doubt about its truth. Nevertheless, it would be all the more worthwhile if anyone could show a rigorous proof of this proposition by which we are more certain of its truth. Indeed, there is no doubt that such a proof, sought in vain for so long, may lead us to many other important properties of the numbers. Although the truth of this proposition is beyond doubt, nevertheless, I will diligently note that I will distinguish the consequences which depend on it from the others which are supported by solid proof; however, from this unproved proposition follow these corollaries which I wish to be designated by that name.

Despite the fact that Euler was one of the most prolific mathematicians ever, he admitted that he doesn't have proof of proposition V but still attempts to prove it. As he stated, two years later "I proved many properties which such numbers are endowed with: it was not permitted to prolong adequately my thoughts about this so that I could show for certain the truth of this theorem, which Fermat once proposed to be proved via geometry. Nevertheless, I then published an attempt at the proof, from which the certainty of this theorem shines much brighter, although it is lacking, according to the criteria of a rigorous proof: I did not doubt that by continuing in the same path, the desired proof could be more easily be obtained, which indeed since that time came to me with experience, so that the attempt, if some other slick idea appears, may become a rigorous proof." [8, paragraph 1]

Fermat did not receive much credit for his number theory work because the topic was too abstract at that time. However, he did lay a foundation for modern number theory and by attracted Euler's attention, one of the most brilliant scientific minds at that time. Thus, Euler went further on number theory where he published many theorems. But number theory, which is founded on prime numbers continues to offer challenges even ones simple to state. As Leonhard Euler said, "Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate." [5]

References

1. Cunningham, A., The Messenger of Mathematics, volume 20, 1890-1, pp. 37-45
2. Dickson, L.E. (1952) *History of the theory of numbers. New York, NY: Chelsea Pub. Co.*
3. *Euclidean algorithm* (no date) *Encyclopædia Britannica*. Encyclopædia Britannica, inc. Available at: https://www.britannica.com/science/Euclidean-algorithm (Accessed: May 6, 2023).
4. *Factorization* (2023) *Wikipedia*. Wikimedia Foundation. Available at: https://en.wikipedia.org/wiki/Factorization#:~:text=Factorization%20was%20first%20considered%20by,into%20integers%20greater%20than%201. (Accessed: May 6, 2023).
5. *Leonhard Euler quotes (author of elements of algebra)* (no date) *Goodreads*. Goodreads. Available at: https://www.goodreads.com/author/quotes/186483.Leonhard_Euler (Accessed: May 6, 2023).
6. Libretexts (2021) *1.2: Factoring, Mathematics LibreTexts*. Libretexts. Available at: https://math.libretexts.org/Bookshelves/Algebra/Book%3A_College_Algebra_and_Trigonometry_(Beveridge)/01%3A_Algebra_Review/1.02%3A_Factoring#:~:text=This%20section%20will%20review%20three,factoring%20a%20Difference%20of%20Squares. (Accessed: May 6, 2023).
7. News, D. (2012) *A brief history of numbers and counting, part 1: Mathematics advanced with Civilization, Deseret News*. Deseret News. Available at: https://www.deseret.com/2012/8/5/20505112/a-brief-history-of-numbers-and-counting-part-1-mathematics-advanced-with-

civilization#:~:text=Numbers%2C%20and%20counting%2C%20began%20about,up%2C%20added%20to%20or%20traded. (Accessed: May 6, 2023).

8. Euler, Leonhard, *On numbers which are the sum of two squares* (1758). Available at: http://eulerarchive.maa.org/docs/translations/E228en.pdf (Accessed: May 6, 2023).
9. *Pierre de Fermat* (no date) *Encyclopædia Britannica*. Encyclopædia Britannica, inc. Available at: https://www.britannica.com/science/number-theory/Pierre-de-Fermat (Accessed: May 6, 2023).
10. *Pierre Fermat - quotations* (no date) *Maths History*. Available at: https://mathshistory.st-andrews.ac.uk/Biographies/Fermat/quotations/ (Accessed: May 6, 2023).
11. Euler, Leonhard, *Proof of a theorem of Fermat that every prime number of the form 4n+1* ... (1760). Available at: https://scholarlycommons.pacific.edu/cgi/viewcontent.cgi?filename=1&article=1240&context=euler-works&type=additional (Accessed: May 6, 2023).
12. Sinclair, J. (2022) *What is the history of factoring?*, *Trade Finance Global*. Available at: https://www.tradefinanceglobal.com/posts/what-is-the-history-of-factoring/ (Accessed: May 6, 2023).