

The Life and Mathematical Contributions of Pierre de Fermat

I. Birth and Upbringing

“Descartes called him a ‘braggart,’ Pascal termed him ‘the greatest mathematician in all of Europe,’ Mersenne referred to him as ‘the learned councillor from Toulouse,’ and Wallis thought of him as ‘that damned Frenchman.’” [7, p. 15] Indeed, Pierre de Fermat was well known throughout all of Europe. He was born in France in 1601, the son of a leather-merchant. He was educated at home and in 1631, he obtained the post of “councillor for the local parliament at Toulouse, and he discharged the duties of the office with scrupulous accuracy and fidelity.” [1, p. 1]. He married later that year and subsequently fathered five children. [7, p. 16] Mathematics, then, was an effort for his leisure time.

He published almost none of his results and has become somewhat of a legend for having routinely given “no systematic exposition of his methods.” [1, p. 1] Some of his more impressive results were found only after his death on loose sheets of paper or written in the margins of works (he seemed to have an affinity for this method of recording his discoveries) which he had read and annotated. “He was constitutionally modest and retiring, and does not seem to have intended his papers to be published.” [1, p. 1]

II. Mathematical Contributions

Probability:

Fermat’s investigations in probability were provoked by requests from his contemporary Blaise Pascal. Pascal posed the following scenario: “Suppose a player has wagered to cast a given number, say 6, with a single die in eight throws, and suppose that after three [unsuccessful] throws, the game is interrupted. How are the stakes to be divided.” [7, p. 402] Fermat’s response was elegant and correct:

On each throw, the chances of success are 1 in 6. Suppose, then, on the one hand, that after the stakes have been met, we agree that I do not make the first throw; then by my principle, I should receive $1/6$ of the stakes as fair compensation. Having made settlement, Fermat continues, and having left the remainder in the pot, suppose we agree that I will not make my second cast; then I receive again $1/6$ of the stakes remaining, i.e. $1/6$ of $5/6$, or $5/36$ of the original stakes. If we continue in this fashion, it is clear that my fourth cast will be worth $125/1296$ of the original stakes...Thus, if my partner proposes that I do not make my fourth throw and wants to compensate me for the chance that I might succeed, he owes me $125/1296$ of the total sum of the stakes. [7, p. 402-3]

Pascal agreed with Fermat's analysis and subsequently sent another problem for Fermat to solve: Two players wager on a series of win-or-lose decisions (such as flipping a coin), in which each player has an equal chance of success. "The first player to win a given number of decisions, say three, wins the stakes. In the event the game is prematurely ended, how should the stakes be divided?" [7, p. 403] Included in Pascal's letter was his solution to the problem:

It is necessary to say first, that if one has made one out of five plays, and hence four are lacking, the game will be completely decided in eight plays, i.e. in twice four plays.

The value of the first of five plays [in terms of the claim] on the opponent's money is the fraction that has as its numerator one half of the combinations of 8 taken $n = 4$ at a time (I take 4 because it is equal to the number of plays lacking, and 8 because it is twice 4), and as its denominator this same numerator plus all superior combinations [Pascal showed that this denominator would always be equal to 2^{2n-1} ; his solution in this case gives $\frac{1}{2} \cdot \frac{{}_{2n}C_n}{2^{2n-1}} = \frac{1}{2} \cdot \frac{{}_8C_4}{2^7} = \frac{35}{128}$]. [7, p. 406]

Fermat agreed with Pascal's solution, but did not care for the method. Fermat wrote:

Consider a game of n plays, which is interrupted after the first play. The winner of that play needs $n - 1$ more wins to gain the entire stakes. Were the game to continue, then, it would be decided in at most $2n - 2$ plays. Since the game consists of a series of independent win-or-lose decision of equal probability, those $2n - 2$ plays have 2^{2n-2} possible outcomes. How many of those outcomes would be favorable to the winner of the first play, i.e. how many would award the whole game to him? The answer, clearly, is any outcome that involved $n - 1$ or more wins for him. To find the number of these favorable outcomes, compute then the number of combinations of $2n - 2$ things taken $n - 1$ at a time, the number of $2n - 2$ taken n at a time, the number taken $n + 1$ at a time, and so on up to the number taken $2n - 2$ at a time. The sum just mentioned is clearly $2^{2n-3} + \frac{1}{2}({}_{2n-2}C_{n-1})$. On the principle, then, that the winner of the first play is entitled to the portion of the entire stakes corresponding to the ratio of the number of outcomes favorable to him to the number of total possible outcomes, he should receive

$\frac{2^{2n-3} + \frac{1}{2}({}_{2n-2}C_{n-1})}{2^{2n-2}}$ of the entire stakes. [7, p. 406-7]

“To see that Fermat’s result agrees completely with Pascal’s, one only need rewrite it in the form $\frac{1}{2} + \frac{1}{2} \left[\frac{{}^{2n-2}C_{n-1}}{2^{2n-2}} \right]$ and recall that Pascal’s result spoke of the portion of the opponent’s ante due the winner, i.e. the portion of $\frac{1}{2}$ the entire stakes. [7, p. 406-7]

After settling this matter, Fermat tried to turn Pascal’s attention to number theory. As will be shown later, Pascal was uninterested in Fermat’s other endeavors. Because of Fermat’s other agenda, their exchanges on probability were relatively brief. “Short lived as it was, it helped lay the foundations of the theory of probability.” [7, p. 410] Neither man, however, went on to develop more of the concepts of probability: Pascal had finished with mathematics and as will be shown, Fermat was to spend his time on number theory. “It was thus left to van Schooten and his pupil Huygens to pick up where Pascal and Fermat had left off and to develop further the classical foundations of probability.” [7, p. 410]

Algebra > Maxima / Minima and Tangents:

Fermat spent much of his early years studying properties of polynomials and rational functions. He developed a method to find the maximum value of $x(a - x)$. His method is essentially equivalent to taking a consecutive value of x , namely $x - e$, where e is very small, and putting $x(a - x) = (x - e)(a - x + e)$. Simplifying, and ultimately getting $e = 0$, we get $x = \frac{1}{2}a$. This value of x makes the given expression a maximum. Of course, what Fermat had developed was an early version of the first derivative test. He had similar methods for finding the minimum value of a function and for finding the slope of a tangent line to a curve at a given point. [1, p. 5]

Number Theory:

Fermat’s contributions to the field of Number Theory are astounding. They become even more significant when the reader is reminded that Fermat lived in an age with no calculators or electronic computing devices. Notwithstanding these limitations, Fermat knew a lot about the properties of the integers. A discussion of several of his results in this area follows.

Number Theory > Aliquot Parts:

He spent a great deal of time studying the properties of the aliquot parts, or proper divisors, of the natural numbers. It was known to the Greeks that 220 and 284 were a pair of “friendly,” or amicable, numbers. In modern notation, using the number theoretic function sigma, we write $\sigma(220) = 284$ and $\sigma(284) = 220$ to illustrate this property. Until Fermat, no one had been able to demonstrate the existence of another pair of friendly numbers. Fermat showed that 17296 and 18416 are also friendly. But more than this, Fermat claimed to have a general solution. He boasted to Mersenne: “I can solve all problems concerning aliquot parts, but the

length of the computations dissuades me, as does the determination of prime numbers, to which all these problems reduce.” [7, p. 220]

Fermat did indeed have a general solution. He noted that if each of $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$, and $r = 3^2 \cdot 2^{2n-1} - 1$ are prime, then $2^n pq$ and $2^n r$ are amicable numbers. This method produces p , q , and r prime when $n = 1, 2, 4$, and 7 . Fermat surely knew that when $n = 1$ the two numbers (34 and 20) are not amicable but he failed to mention such in his letter to Mersenne, perhaps dismissing the counterexample as obvious. The following table shows the amicable numbers generated for $n = 2, 4$, and 7 . Fermat is generally credited with the case $n = 4$, while Descartes is credited with the case $n = 7$. These are the only three pairs of amicable numbers that can be found by this algorithm for $n < 20000$ [9]

n	Amicable pair	n	Amicable pair
2	284 and 220	7	9,437,056 and 9,363,584
4	18,416 and 17,296		

Euler later used a different method to add 62 new pairs of amicable numbers. He thus showed that Fermat’s method did not generate all pairs of amicable numbers. Nicolo Paganini, a sixteen-year old Italian boy, discovered the second smallest pair (1184 and 1210) in 1866. Today, extensive computer searches have found all such numbers with 10 or fewer digits and numerous larger examples, for a total of over 7500 amicable pairs. It is unknown if there are infinitely many pairs of amicable numbers. It is also unknown if there is a relatively prime pair of amicable numbers. If there is such a pair, they must be more than twenty-five digits long, and their product must be divisible by at least 22 distinct primes. [2]

Fermat was also interested in a certain subclass of the “deficient” numbers – those for which the sum of the aliquot parts is an integral multiple of the number. For example, $\sigma(672) = 1344 = 2 \cdot 672$. Fermat also gave a general solution for this problem. He noted that if

$p = \frac{2^n - 1}{2^{n-3} + 1}$ is prime, then $q = 2^{n-1} \cdot 3p$ is equal to one half the sum of its aliquot parts. That is, $\sigma(q) = 2q$. [7, p. 292] For $n < 5000$, p is only an integer twice – namely when $n = 4$ and when $n = 6$. When $n = 4$, $p = 5$, and $q = 120$. When $n = 6$, $p = 7$, and $q = 672$. It follows then that $\sigma(120) = 240 = 2 \cdot 120$ and $\sigma(672) = 1344 = 2 \cdot 672$.

It is unfortunate that “none of Fermat’s extant writings offers the slightest hint of how he derived these general formulas and other specific solutions of aliquot part problems; cf., for example,

Fermat to Mersenne...where he gives $\sigma(2016) = \left(\frac{9}{4}\right) \cdot 2016$ and he identifies a solution of enormous size for the equation $\sigma(x) = 5x$.” [7, p. 292]

Fermat's general solutions to the questions of aliquot parts led to a correspondence with the French mathematician Bernhard Frénicle de Bessy (1605-1675), who was intrigued by Fermat's results. Frénicle was an official at the French mint who was renowned for his gift of manipulating large numbers. On one occasion, he heard that Fermat had proposed the problem of finding cubes, which when increased by their aliquot parts, become squares (as is the case with $7^3 + 1 + 7 + 7^2 = 20^2$). He immediately gave four different solutions and supplied six more the next day. [2, p. 88]

This correspondence lasted for the better part of twenty years and has proved to be important to historians because Frénicle's questions / challenges regarding number theory drew out of Fermat some of his carefully guarded methods and procedures. Thus, "their correspondence is perhaps the most valuable source of information about Fermat's number theory." [7, p. 293]

In March 1640, Frénicle sent Fermat his first challenge – to find a perfect number of twenty or twenty-one digits. It was a well known result of Euclid that if $2^n - 1$ was prime, then $2^{n-1} \cdot (2^n - 1)$ was perfect. So Frénicle's challenge was really a challenge to check the primality of $2^n - 1$ for large values of n . The problem could not be done using the Sieve of Eratosthenes because of the sheer size of $2^n - 1$. Despite this limitation, Fermat responded almost immediately: "I have several shortcuts for finding perfect numbers, and I can say in advance that there is none of 20 digits, nor any of 21 digits..." [7, p. 294]. Hence Fermat provided a counterexample for the widely held belief that each decimal interval (from 10^n to 10^{n+1}) contained one perfect number. This result did not surprise Frénicle – he was already aware of the result when he sent his challenge to Fermat. He was intrigued, however, by Fermat's reference to his "several shortcuts" and he asked Mersenne to probe further into the matter.

Fermat's response to Mersenne's inquiry makes some of his methods more clear. Before explaining Fermat's methodology, it is necessary to make the reader familiar with some of Fermat's terminology. He referred to the number $2^n - 1$ as the "radical" of the perfect numbers, since each prime in the sequence of radicals uniquely determines a perfect number. Fermat gave Mersenne three propositions that reduced the primality of any radical to the primality of its index n .

Fermat's first proposition: if n is composite, then $2^n - 1$ is composite.

Proof: The proof is algebraic. Notice that $a^{pq} - 1 = (a^p - 1) \cdot (a^{p(q-1)} + a^{p(q-2)} + \dots + 1)$. This completes the proof.

Fermat's second proposition: if n is prime, then $2n$ divides $2^n - 2 = (2^n - 1) - 1$.

Equivalently, if n is prime, then $n \mid 2^{n-1} - 1$.

Proof: The proof follows directly from Fermat's Little Theorem, which will be stated hereafter.

Fermat's third proposition: if n is prime, then the only possible divisors p of $2^n - 1$ are of the form $p = k(2n) + 1$.

Proof: The proof also follows from Fermat's Little Theorem, but requires more arguments than Fermat's second proposition. The proof will be given hereafter.

Fermat said nothing about how each proposition was known to be true beyond saying that they had been found "not without difficulty." [7, p. 294] Fermat used his first and third propositions to answer Frénicle's challenge. He first noticed that the only possible perfect number of twenty or twenty-one digits corresponds to $2^{37} - 1$ since the index n of the radical for all other candidates of the appropriate size is composite (the reader will notice that 32, 33, 34, 35, 36, 38, 39, and 40 are all composite). The first proposition then implies that the radical is composite for all of these cases. Fermat then used his third proposition to show that $2^{37} - 1$ is divisible by $223 = 3(2 \cdot 37) + 1$. It was this shortcut that enabled Fermat to respond so quickly to Frénicle's challenge.

Fermat concluded his letter to Mersenne by writing, "from these shortcuts, I already see a great number of others emerging, and for me it is like seeing a great light." Mahoney notes:

Fermat was just being coy. He had already seen the light, and his three propositions were merely faint rays of it...Of the three propositions, the two concerning prime n were merely corollaries of a far more general theorem that Fermat announced directly to Frénicle on 18 October 1640 and that he must have already had at hand much earlier. [7, p. 294-5]

The theorem, which is known today as Fermat's Little Theorem, was first stated in the following form: "given a prime p and a sequence of numbers of the form $a^t - 1$ (t a positive integer), then p divides some least member of the sequence, say $a^T - 1$ and $T \mid p - 1$; moreover, p also divides all members $a^{kT} - 1$ ($k = 1, 2, \dots$) of the same series." [7, p. 295] Fermat wrote that the result was true in general for all series and all prime numbers and would have sent a demonstration had he not feared "going on for too long." [7, p. 295]

The usual form of Fermat's theorem today is: if p is prime, and a is any integer relatively prime to p (Fermat did not include this condition in his version of the theorem), then $a^{p-1} = 1 \pmod{p}$. Using modern notation, we can restate Fermat's version as: there exists a least integer t such that $a^t = 1 \pmod{p}$ and $t \mid p - 1$. To show this is equivalent to the modern version, notice that $t \mid p - 1 \Rightarrow p - 1 = kt$. Since $a^t = 1 \pmod{p}$, $a^{kt} = 1 \pmod{p}$ as well. Substitution yields the desired result: $a^{p-1} = 1 \pmod{p}$.

The proof is not difficult and the interested reader is referred to any number theory text. Clearly, Fermat had proved his theorem; but he never published it. Euler gave the first published proof in 1736 – almost one hundred years after Fermat revealed the theorem to Frénicle – and gave a generalization (of which Fermat's Little Theorem is a corollary): If n is a positive integer and $\gcd(a,n) = 1$, then $a^{\phi(n)} = 1 \pmod{n}$. [8, p. 64] Burton notes that "Leibniz...seems not to have received his share of recognition, for he left an identical argument in an unpublished manuscript sometime before 1683." [2, p. 89]

We now return to give proofs of Fermat's second and third propositions. For convenience, the propositions are restated.

Fermat's second proposition: if n is prime, then $2n$ divides $2^n - 2 = (2^n - 1) - 1$.

Equivalently, if n is prime, then $n \mid 2^{n-1} - 1$.

Proof: This proposition is just simply Fermat's Little Theorem for n a prime and $a = 2$. Notice that $n \mid 2^{n-1} - 1 \Rightarrow 2^{n-1} = 1 \pmod{n}$.

Fermat's third proposition: if n is prime, then the only possible divisors p of $2^n - 1$ are of the form $p = k(2n) + 1$.

Proof: Suppose n is prime but $2^n - 1$ is composite. Then by the Fundamental Theorem of Arithmetic, $2^n - 1$ is divisible by some odd prime p ($2^n - 1$ is odd so it cannot be divisible by two). By his theorem, Fermat knew that $n \mid p - 1$, which implies $p - 1 = k'n$ for some integer k' . Since p is odd, $p - 1$ is even. Then $2 \mid p - 1 \Rightarrow 2 \mid k'n$. Since n is prime, 2 does not divide n . Thus, $2 \mid k' \Rightarrow k' = 2k$. Therefore, $p - 1 = 2kn$, or $p = k(2n) + 1$. [7, p. 297]

At this point, an example to show the power of Fermat's Theorem would be appropriate. Suppose it was necessary to know the remainder when 7^{1015} was divided by 31. That is, we want to calculate $7^{1015} \pmod{31}$. By Fermat's theorem, we know that $7^{30} = 1 \pmod{31}$. Since $1015 = 30 \cdot 33 + 25$, $7^{1015} \equiv 7^{30 \cdot 33 + 25} \equiv 1^{33} \cdot 7^{25} \equiv 7^{25} \pmod{31}$. To calculate $7^{25} \pmod{31}$, we first calculate $7^n \pmod{31}$ for $n = 2, 4, 8$, and 16. This gives: $7^2 \equiv 49 = -13 \pmod{31}$, $7^4 \equiv 169 = 14 \pmod{31}$, $7^8 \equiv 196 = 10 \pmod{31}$, and $7^{16} \equiv 100 = 7 \pmod{31}$. It follows then that $7^{25} \equiv 7 \cdot 7^8 \cdot 7^{16} = 7 \cdot 10 \cdot 7 \equiv 490 \equiv 25 \pmod{31}$

As has been noted, Fermat spent a lot of time thinking about prime numbers. It should not be surprising then, that he was found to be looking for certain forms that always produced prime numbers. Fermat conjectured, for example, that $F_n = 2^k + 1$, where $k = 2^n$ is prime for all $n \geq 1$. Fermat announced this conjecture in a letter dated August 1640 to Frénicle by writing: "I am just about convinced that all progressive numbers augmented by unity, or which the exponents

are numbers of the double progression, are prime numbers...I do not have an exact proof of it, but I have excluded such a large quantity of divisors by infallible demonstrations, and my thoughts rest on such clear insights, that I can hardly be mistaken.” [7, p. 301]

Evidence suggests that Fermat “bemoaned his inability to find a proof, and his tone of growing exasperation suggests that he was continually trying to do so.” But the proof would never come; for, as Euler showed in 1732, F_5 is divisible by 641. Today, F_n is generally been referred to as the n^{th} Fermat number. When F_n is prime, then it is referred to as a Fermat prime. Modern computers have helped establish the primality of F_n for $0 \leq n \leq 4$ and the compositeness of F_n for $5 \leq n \leq 31$. [4].

The Fermat primes later proved to be quite important in solving one of the three Greek problems from antiquity. Gauss showed that a regular polygon of n sides could be inscribed in a circle with classical Euclidean tools if and only if n is a power of two times a product of distinct Fermat primes. [4] Recently, some mathematicians have become interested in the properties of Generalized Fermat primes. Instead of using 2 as the base, Generalized Fermat primes vary the base; so $GF(n, b) = b^k + 1$, where $k = 2^n$. In June 2000, $GF(16, 48594) = 48594^{65536} + 1$ was shown to be prime. $GF(16, 48594)$ has several interesting properties: it is the largest known Generalized Fermat prime, is the largest known prime which is not a Mersenne prime, and is the sixth largest prime known. [6] The top twenty Generalized Fermat primes have all been discovered in the year 2000 or the year 2001. [5]

Number theory > Rational Triangles:

As with aliquot parts, perfect numbers, and prime numbers, the topic of rational right triangles belonged to the traditional problems of the seventeenth century. “And, just as Fermat’s treatment of the former subject led to the foundation of an entirely new sort of arithmetic, the sort inherent in his theorem, so too his approach to rational right triangles eventually reshaped the subject itself.” [7, p. 302]. Mahoney comments on Fermat’s achievements in this area:

Here his achievement was twofold: on the one hand, he extended the effectiveness of traditional solution techniques, and was thereby able to solve problems his predecessors and contemporaries thought impossible; on the other hand, he used rational right triangles and their techniques to attack a body of problems apparently unrelated to them and in doing so created a body of number theory that has outlived its source. Starting from triangles, Fermat arrived at theorems concerning the decomposition of numbers into sums of squares and at his first method for generating complete solutions to the so-called ‘Pell Equation...’ [The subject] appears in his earliest correspondence and becomes the focus of his exchange with Frénicle from 1641 on...What number theory Fermat does after 1657 belongs unmistakably to the new tradition of which he is the founder. [7, p. 302]

The study of rational right triangles refers to triples of rational numbers x , y , and z satisfying the relationship $x^2 + y^2 = z^2$. In his text *Arithmetic*, Diophantus discussed such problems at length and provided the techniques used to solve them. Diophantus' techniques, however, did not always fulfill their promise. His methods occasionally led to a negative rational solution. Not knowing how to deal with such a problem (the length of a side of a triangle cannot be negative), Diophantus and all mathematics up to Fermat declared such a problem unsolvable. Fermat, however, knew otherwise. In a 1643 letter to Frénicle, Fermat posed three problems:

1. Find a right triangle such that the hypotenuse is a square and the sum of the two perpendiculars is also a square
2. Find four right triangles having the same area
3. Find a right triangle such that the area plus the square of the sum of the smaller sides is a square.

Almost immediately, Frénicle responded with "anger and distrust" because he thought Fermat had posed an impossible set of problems. [7, p. 307] Fermat assured him that the problems had solutions, and eventually he supplied them. Consider the third problem: let the two smaller sides of the desired triangle be x and 1. Then the square of their sum, plus the area, set equal to a square yields: $x^2 + \frac{5}{2}x + 1 = y^2$. Moreover, it also necessary that $x^2 + 1^2 = z^2$ for some positive rational number z . The problem with this example is that the usual application of the Diophantine method provides a negative rational solution. Fermat had discovered how to extend the Diophantine method in such a way that enabled him to solve such problems. Indeed, he knew how to obtain a positive rational solution when a negative one appeared first. "His discovery, perhaps first made in the early 1640s, reveals not only the secret of his total mastery over the field of rational right triangles but also the manner in which the model of the theory of equations influenced his thinking in the realm of number theory as it had in geometry." [7, p. 308]

Fermat eventually gave the solutions. The triple (1061652293520, 4565486027761, 4687298610289) satisfies the conditions in problem one. Indeed, $4687298610289 = 2165017^2$ and $1061652293520 + 4565486027761 = 2372159^2$. [10, 125; 10, 620-621] The four right triangles needed in problem two are: ?? And the right triangle for number three is: ?????

Using the same method, Fermat was able to provide a solution to a problem that Frénicle, being himself unable to solve the problem, had asked Fermat to solve. The problem was to find a triangle in which the square of the difference of the two perpendiculars exceeded twice the square of the smaller side by a square number. As discussed above, this problem was thought to be unsolvable because it rendered a negative answer when Diophantus' method was used to solve it. Fermat, however, showed that the triple (156, 1517, 1525) satisfies the given conditions. Indeed, $(1517 - 156)^2 - 2 \cdot 156^2 = 1343^2$. [7, p. 312]

Number Theory > Primality Testing and Integer Factorization:

One of the attributes that distinguished Fermat from his contemporaries was his ability to show that problems of a seemingly limited nature actually had a far wider range of applicability. A classic example of this is a problem that Fermat posed to Mersenne and Frénicle: given a number N , determine the number of different [right] triangles of which it is one of the smaller sides. Fermat later announced the solution:

Every non-square odd number...is the difference of two squares as many times [i.e. in as many ways] as it is composed of two numbers. If the squares are mutually prime, the numbers composing them will also be prime. But if the squares have a common divisor, the number in question will also be divisible by the same common divisor, and the numbers composing the squares will be divisible by the root of that common divisor. [7, p. 325]

Fermat offered an example as his proof. Let $N = n_1 n_2$ be an odd number. Then both factors are also odd and $\left[\frac{n_1 + n_2}{2}\right]^2 - \left[\frac{n_1 - n_2}{2}\right]^2 = n_1 n_2 = N$. Fermat then announced the solution to the problem: "Clearly, the number of different pairs of squares of which N represents the difference depends on the number of different pairs of odd factors of which N is composed." [7, p. 326] A lesser mathematician might have found this result relatively easily and then moved on to more difficult problems. But Fermat saw that there was more that could be done with this result.

In a separate letter, he asks, "let a number, e.g. 2027651281, be given me and let it be asked whether it is prime or composite, and, in the latter case, of what numbers it is composed." [7, p. 326] Fermat's solution was as follows: suppose N is composite and that $N = n_1 n_2$. Then by the above result, there exist integers x , and y such that $x^2 - y^2 = N$. Rewrite that equation in the form $x^2 - N = y^2$, and then find the integer m such that $m^2 < N < (m+1)^2$. In more modern notation, $m = \lfloor \sqrt{N} \rfloor$ (the floor of the square root of N). Then check to see if $(m+1)^2 - N$ is a perfect square. If it is not, check $(m+2)^2 - N$. In checking to see if the number is a square, Fermat noted that certain numbers can be eliminated right away just by examining the last digit of the number. Fermat had noticed that a square must end in one of the six digits 0, 1, 4, 5, 6, or 9. For large N , it might be helpful to make a table of square modulo one hundred. There are only 22 possibilities for the last two digits of any square number. In this manner, 78% of possible squares can be eliminated without doing any computations. [2, p. 86]

Continue increasing m by one until you find $(m+k)^2 - N = n^2$. Then you know that $N = (m+k+n)(m+k-n)$. Clearly, the process cannot go on forever since you will eventually

arrive at the trivial factorization $N = N \cdot 1$. If this happens, then N is prime. Fermat wrote that the total number of test values for k will not exceed $\frac{N - 2m + 1}{2}$.

Burton notes that Fermat's method is "most effective when the two factors of n are of nearly the same magnitude, for in this case, a suitable square will appear quickly" and he gives an example. Suppose we are to factor $n = 23449$. Here, $m = 153$. Now perform the computations:

$$154^2 - 23449 = 23716 - 23449 = 267 \neq n^2$$

$$155^2 - 23449 = 24025 - 23449 = 576 = 24^2$$

Hence, the factors of 23449 are:

$$23449 = 155^2 - 24^2 = (155 + 24)(155 - 24) = 179 \cdot 131. \text{ [2, p. 86]}$$

Fermat used this procedure to factor $2027651281 = 44021 \cdot 46061$ in only eleven steps. Burton writes that Fermat probably chose this "favorable case...on purpose to show that chief virtue of his method: It does not require one to know all the primes less than \sqrt{n} in order to find factors of n . Fermat's factoring algorithm was the first to improve upon the Sieve of Eratosthanes and it remained the algorithm of choice for hundreds of years to follow.

Number Theory > Primes and Squares:

Having "laid to rest an old tradition (rational triangles)," Fermat now sought to institute a new one – "arithmetic as the doctrine of whole numbers, or number theory in the modern sense." [7, p. 314] He began this work by responding to a challenge from the French mathematician Bachet. Bachet, noting that any number that can be written as a sum of two squares in two different ways will be the hypotenuse of four different right triangles (its square will be the sum of two squares in four different ways), asked Fermat to find a general solution to this problem. That is, Fermat was to determine which numbers could be written as a sum of two squares in a given number of ways. Bachet was able to offer some specific partial answers, but could not generalize a solution [7, p. 316].

Fermat composed the major portion of the solution in a letter to Mersenne on Christmas Day 1640. He noted:

If a prime number composed of two squares [the prime can be written as the sum of two squares] is multiplied by another prime number also composed of two squares, the product is twice composed of two squares; if it is multiplied by the square of the same prime, the product is composed of two squares in three ways; if it is multiplied by the cube of the same prime, the product is composed of two squares in four ways, and so *in infinitum*. [7, p. 316]

To illustrate Fermat's solution, consider $5 = 1^2 + 2^2$ and $13 = 2^2 + 3^2$. To find a number that is "twice composed of two squares," all that is needed is their product. Indeed, $5 \cdot 13 = 65 = 7^2 + 4^2 = 8^2 + 1^2$. Moreover, $845 = 5 \cdot 13^2$ should be "composed of two squares in three ways." Again, this is the case: $845 = 2^2 + 29^2 = 13^2 + 26^2 = 19^2 + 22^2$. Finally, notice that $10985 = 5 \cdot 13^3 = 13^2 + 104^2 = 28^2 + 101^2 = 52^2 + 91^2 = 64^2 + 83^2$ can be written as a sum of two squares in four ways.

Fermat essentially solved this problem by "reducing the question of the various decompositions of a given number into two squares to that of the various decompositions of its prime factors." [7, p. 316]. He explained his method in his Christmas Day letter:

From this it is easy to determine how many times a given number is the hypotenuse of a right triangle [i.e. can be written as the sum of two squares]. Take all prime numbers exceeding by unity a multiple of four that measure [divide] the given number; e.g. 5,13,17. If powers of the said primes measure the said number, arrange them together with the rest in place of their roots; e.g. let them measure the given number [as follows]: 5 by the cube, 13 by the square, and 17 by the simple root. Take all the exponents of all the divisors; i.e. the exponent of the number 5 is 3 owing to the cube, the exponent of the number 13 is 2 owing to the square, and of the number 17 is unity only. Order, then, as you wish, all said exponents; as, if you will, 3, 2, 1. Multiply the first by [twice] the second...and, adding the product to the sum of the first and the second, the result is 17. Then multiply 17 by [twice] the third...and, adding the product to the sum of 17 and the third, the result is 52. Therefore, the given number will be the hypotenuse of 52 right triangles. The method is no dissimilar for any number of divisors and their powers. The remaining prime numbers [dividing the given number], which do not exceed a multiple of four by unity, add or detract nothing from the question, nor do their powers. [7, p. 318]

The solution of Bachet's problem reduces, therefore, to the determination of which primes uniquely split into the sum of two squares." [7, p. 316-7] As hinted above, Fermat solved this problem as well. He stated its solution in his Christmas Day letter to Mersenne:

A prime number, which exceeds a multiple of four by unity, is only once the hypotenuse of a right triangle, its square twice, its cube three times, its quadratoquadrate four times, and so on *in infinitum*. [7, p. 316]

In modern notation, Fermat had noted that if a prime p is of the form $4k+1$ (i.e. $p \equiv 1 \pmod{4}$), then p is uniquely the sum of two squares. Fermat also knew that primes of the form $4k+3$ could not be written as the sum of two squares. Hence, the number of ways in which the square of a given number can be split into two squares depends only on its prime factors of the form $4k+1$. [7, p. 317]

Finally, Fermat answered the original question posed by Bachet. Recall that Fermat was to find a number that is composed of two squares in a given number of ways. As in the past, Fermat gave the answer without the slightest hint of its derivation: if $N = p^a q^b \dots s^c$ where p, q, \dots, s are all primes of the form $4k+1$ then N may be represented as the sum of two squares in $\frac{1}{2}[(a+1)(b+1)\dots(c+1)]$ ways. “Although the details of Fermat’s solution to Bachet’s question...attest to Fermat’s command of combinatorics, they provide no insight into the origins of the...theorem that makes the combinatorial superstructure possible. They do not, that is, explain how Fermat knew that any prime number of the form $4k+1$ splits uniquely into two squares. [7, p. 320]

From 1644 to 1654, Fermat seemingly broke off his correspondence with Mersenne, Bachet, and Frénicle. Mahoney suggests that this was because the exchanges generated bad feelings: “[they] felt that Fermat was...posing problems that had no solution in order to expose his rivals. Fermat suspected that they, in turn, were siding with those who accused him of relying on clever guesswork.” [7, p. 335]

This period of silence was broken by Pascal’s request for aid in solving a problem in probability. After answering Pascal’s questions, the discussion of which has taken place heretofore, Fermat immediately changed the subject to number theory. Mahoney notes, “the results that Fermat chose from the myriad of his earlier correspondence document conclusively the change his thinking had undergone regarding the nature of arithmetic and the sorts of problems he had been investigating in the interim. ‘I hope to send you on St. Martins’ Day a sketch of everything worthwhile that I have discovered concerning numbers,’ he wrote.” [7, p. 332-3] Fermat made a number of important discoveries during this time period, all of which he revealed to Pascal:

1. Every number is either a triangular number or composed of two or three triangular numbers; a square [number]; or composed of two, three, or four square [numbers]; a pentagonal number or composed of two, three, four, or five pentagonal numbers; and so on indefinitely.
2. Every prime of the form $3k+1$ is composed of a square and the triple of a square.
3. Every prime of the form $8k+1$ or $8k+3$ can be expressed as the sum of a square and the double of a square.
4. No integral right triangle can have a square area (which implies if $a^2 + b^2 = c^2$ then ab cannot be a square either).

“Fermat [was] dangling before Pascal’s eyes the promise of an arithmetic more subtle and powerful than anything the Ancients (or, indeed, the moderns) possessed. [7, p. 333] It seems reasonable to also suggest that by this time, Fermat had a complete solution to the general equation $x^2 - py^2 = \pm q$. But Pascal proved to be uninterested. He wrote to Fermat:

Look elsewhere for someone to follow you in your numerical researches, of which you have done me the honor of sending the statements. As far as I am concerned, I confess to you that they go right past me; I am capable only of admiring them and of begging you very humbly to take the first opportunity to complete them... [7, p. 334]

Thus ended Fermat's correspondence with Pascal. In 1656, Fermat received a copy of Wallis' recently published *Arithmetic of Infinities*. Fermat was impressed with the topic – number theory – but not the results. Fermat considered the work to be substandard; yet he hoped to find Wallis willing to carry on a correspondence. To start things off, Fermat wrote to Wallis by posing two problems: find a cube that, added to all its aliquot parts, makes a square; also sought was a square that, added to all its aliquot parts, makes a cube. "The challenge failed to bring the results Fermat had optimistically expected. He apparently thought that they would lead other mathematicians to the same subject to which they had led him and which had formed the core of his research over the previous dozen years. [7, p. 337]

The first problem calls for the solution $1 + x + x^2 + x^3 = y^2$ for some prime x . Rewrite the left hand side: $(1 + x)(1 + x^2) = y^2$, where each of the factors is even. However, they have only the factor two in common and are otherwise relatively prime. Thus, $y^2 = 2u^2 + 2v^2$, with $\gcd(u^2, v^2) = 1$. It follows then that $x = 2u^2 - 1$ and $x^2 = 2v^2 - 1$.

"Fermat was prepared to show, as he later did, not only that the general form of these equations, i.e. $2u^2 - w^2 = p$, has solutions if and only if p is a prime of the form $8k \pm 1$ or contains prime factors of that form, but that the special cases to which the first challenge problem reduced have solutions only for the prime 1 and 7 and no others." [7, p. 337-8] For $x = 7$, we have $7^3 = 343 + 1 + 7 + 49 = 400 = 20^2$.

Wallis seemingly brushed off Fermat's attempt at correspondence and never showed much interest in Fermat's future challenges. Fermat continued to send Wallis problems to solve:

1. Prove that (5,3) is the only solution to $x^2 + 2 = y^3$.
2. Prove that (2,2) and (11,5) are the only solutions to $x^2 + 4 = y^3$.
3. Prove that the double of every prime of the form $8k + 1$ can be expressed as the sum of three squares.
4. Prove that the product of any two primes of the form $20k + 3$ or $20k + 7$ can be expressed as the sum of a square and five times a square.
5. Prove Diophantus' conjecture: any number can be expressed as the sum of at most four squares.

Wallis never replied. "Fermat had again lost by winning...No one was prepared to assist Fermat in restoring the pure doctrine of whole numbers....Even history has compounded the futility of Fermat's effort. By a mistake of Euler's...the equation $y^2 - px^2 = 1$ has gone into the mathematical literature bearing the name of John Pell, whose only contribution was to write it down in his papers." [7, p. 347]

Number Theory > Fermat's Last Theorem:

Any discussion of Fermat's contributions to number theory would be incomplete without mentioning the celebrated "Last Theorem:" the equation $x^n + y^n = z^n$ has no integer solutions for $n > 2$. Previous examples have shown that Fermat was often unwilling to give proofs of statements. But his statement with respect to the last theorem has transcended them all: "I have discovered a truly remarkable proof which this margin is too small to contain." It now seems likely that Fermat was convinced of the truth of the statement for $n = 3$ and $n = 4$ and being confident that he could adapt them to any exponent, he never really dealt with $n \geq 5$. Even Euler was unable to provide a proof for $n = 5$. [7, p. 358]

Although the "Last Theorem" was not Fermat's last theorem in number theory, Mahoney notes,

it may well serve that purpose here. It sums up Fermat's work in that field. It is shrouded in mystery because Fermat could not or would not find the time to record his "proof" for posterity, or even for himself...Fermat's contributions to number theory, unlike his work in other fields, never slipped into obscurity because the "Last Theorem," together with many others, has hitherto remained a seemingly elementary, intuitively true theorem lacking a proof. Fermat did not live to see his dream of a new tradition in arithmetic realized, but it was. It was, from the day Christian Goldbach first called Leonhard Euler's attention to Fermat's conjecture regarding primes. It was, during the twenty years in which E.E. Kummer devised a complete theory of the complex number field while trying to prove the "Last Theorem". And it has been in [the 20th Century] with the development of modern algebraic geometry, culminating in...a proof of the theorem by Andrew Wiles. [7, p. 358-9]

III. Death and Legacy

Fermat died in 1665. He left a legacy that would not leave the mathematical community unaffected. Indeed, he had been a leader in a movement that

fundamentally altered the practice of mathematics. [He] loosed it from the strict geometric model of classical Greek antiquity and reformulated it in terms of a new algebraic model...Like any art, [mathematics] could not rest content with admiring past masterpieces, but rather had to analyze them to discover how they had been achieved and use them as a starting point for new work. And

where past masters had obscured their techniques, present artists must devise their own. Only in that way could the art progress.” [7, p. 363]

In short, Fermat provided the tangible evidence (none of his contemporaries could) that the “problem-solving benefits of algebraic analysis far outweighed the loss of intuitive understanding that a concrete picture and tactile operations of geometric construction seemed to provide. In doing so, he spoke directly to a new generation of mathematicians for whom utility had become more important than esthetics.” [7, p. 365] In a very real sense, then, we see that Fermat “presided over the death of the classical Greek tradition in mathematics. At that start of his career...the tradition was both alive and thriving...Over his career, however, Fermat moved so far beyond his original sources as to make them obsolete.” [7, p. 365] This becomes increasingly clear when it is noted that while Fermat learned his mathematics from the Greek texts, Newton learned what he knew from Descartes, Fermat, and other ‘modern’ analysts of the day. [7, p. 365]

The accomplishments of Newton and Leibniz did not come in a “fit of unprecedented genius.” [7, p. 362] Rather, the development of the Calculus came as a result of a new approach to mathematics. Notably, they were not the originators of the approach; Fermat was. They were merely the “inheritors and the continuators.” [7, p. 362] One cannot fully understand the significance of their accomplishments without first placing it “in the context of that new approach, a context which transcended the calculus in its importance for the development of modern mathematics.” [7, p. 362-3]

Fermat’s failure to publish his works did not affect his influence on the mathematical community. People clearly talked about him. His failure to publish would only affect him in one way – in the history books; that is, the mathematics he developed would in so many cases be severed from his name:

It meant that Beau grand would pass off the method of tangents as his own...It means that Johann Hudde would embellish the method of maxima and minima and claim it as his own invention...It meant ultimately that the fundamental algorithm of the *Method of Maxima and Minima* would go down in history as ‘De Sluse’s Rule.’ And Fermat would be forgotten. Analytic geometry would be called ‘Cartesian,’ the second-derivative characteristic for extreme values would be anonymous, even the equation $px^2 - y^2 = \pm 1$ would acquire the title ‘Pell’s Equation.’ Only number theory would remain Fermat’s undisputed province; and it would do so ironically, because Fermat could interest none of his contemporaries in it. [7, p. 365-6]

Despite the immediate obscurity into which Fermat’s name fell, in retrospect, his effect on the development of mathematics in the seventeenth century is clear:

It extended beyond the technical content and outward style of mathematics to touch the very way in which men came to think about the subject, and beyond that to the manner in which they practiced it...

Algebraic analysis...became the mathematics of the Academy of Sciences in Paris and the new Imperial Academy in St. Petersburg. It filled the pages of the mathematical journals. It formed the common language of Continental mathematics by the early decades of the eighteenth century and hence the language anyone who would be called a mathematician had to command...

Hence, the career of Fermat illustrates more than mathematics in transition; it reveals the mathematician in transition. With Leibniz, Fermat was one of the last great mathematicians to pursue the subject as a sideline to an essentially non-scientific career...The explosive growth of the subject, which he played such an important role in releasing, entailed the increasing specialization of mathematical research and...the necessity for formal training...In retrospect, Fermat's achievement meant the end of men like himself. It placed mathematics beyond the point where a provincial lawyer far removed from a center of scientific activity could, on his own, and in his spare time, make fundamental advances, and thus it set the boundaries that would increasingly separate the professional from the amateur in mathematics." [7, p. 366-7]

References:

1. Ball, W.W. Rouse. A Short Account of the History of Mathematics, 4th ed. Published 1908.
http://www.maths.tcd.ie/pub/HistMath/People/Fermat/RouseBall/RB_Fermat.html
2. Burton, David. Elementary Number Theory, 4th ed. New York: McGraw-Hill, 1997.
3. Caldwell, Chris. "Amicable Numbers." <http://www.utm.edu/research/primes/glossary/AmicableNumber.html>
4. Caldwell, Chris. "Fermat Primes." <http://www.utm.edu/research/primes/glossary/Fermats.html>
5. Caldwell, Chris. "The Top Twenty Generalized Fermat Primes." <http://www.utm.edu/research/primes/lists/top20/GeneralizedFermat.html>
6. Gallot, Yves. "Generalized Fermat Prime Search." <http://perso.wanadoo.fr/yves.gallot/primes/gfn.html>
7. Mahoney, Michael Sean. The Mathematical Career of Pierre de Fermat, 2nd ed. Princeton: Princeton University Press, 1994.

8. Shockley, James. Introduction to Number Theory. New York: Holt, Rinehart, Winston, 1967.
9. Winkler, Martin. "Friendly Numbers." <http://www.crosswinds.net/~martinwinkler/friendly.html>
10. Dickson, L.E. History of the Theory of Numbers. Washington, DC: Carnegie Institution, 1919-1923), reprint (New York: Chelsea Publishing Co., 1992), Vol. II.