# 6.7. More on Prime Numbers

**Note.** In this section, we explore Fermat numbers and give some of their history. We give two more proofs that there are infinitely many primes, one based on analytic number theory (which we very briefly discuss).

**Definition.** A natural number of the form $F_n = 2^{2^n} + 1$ is a *Fermat number*. For $n \in \{0, 1, 2, 3, 4\}$ we have$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65{,}537$; each of these are prime and are called the *Fermat primes*.

**Note.** Pierre de Fermat (August 17, 1601–January 12, 1665) was a French lawyer, government official, and amateur mathematician.

Pierre de Fermat (August 17, 1601–January 12, 1665),
image from Fermat's Library website.

He was friends with several mathematicians of his time and he corresponded with

many others. He was recognized as a top mathematician, but he did not bother to give clean, clear proofs of his ideas and he did not publish his work (though some of his ideas made it into publication as supplements to the work of others). A more detailed biography can be found in my online notes for Elementary Number Theory (MATH 3120) on Section 6. Fermat's and Wilson's Theorems. Fermat thought that all "Fermat numbers" were in fact prime. His correspondence on this is detailed in Raymond Archibald's "Remarks on Klein's 'Famous Problems of Elementary Geometry'," *The American Mathematical Monthly*, **21**(8), 247–259 (October 1914). A copy is available through JSTOR (accessed 2/26/2022). In August 1640 Fermat wrote to French mathematician Bernard Frénicle de Bessy that "...here is something which pleases me greatly: it is that I am almost persuaded that numbers of the progression $2^{2^0}$, $2^{2^1}$, $2^{2^3}$, ..., augmented by 1, are prime numbers, as 3, 5, 17, 257, 65537, 4,294,967,297...I have not an exact demonstration, but I have excluded such a large number of divisors by infallible proofs, and have so many side lights which bear out my thought, that I would find difficulty in convincing myself of error." In October 1640 he wrote de Bessy again that "I have no more doubt at this moment than I had previously." Fermat wrote to Blaise Pascal 14 year later on August 29, 1654 when he expressed a bit of frustration: "The demonstration of the proposition is very difficult and I confess to you that I have not yet fully found it; I should not propose that you seek it, had I already reach the goal." The difficulty of manipulating such large numbers (by hand) is reflected in the fact that it wasn't until 1832 that Leonhard Euler (April 15, 1707–September 18, 1783) showed in his first number theory publication that $F_5$ is composite and that $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4{,}294{,}967{,}297 = 41 \times 6{,}700{,}417$. He published

his result as "Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus," *Commentarii Academiae Scientiarum Petropolitanae*, **6**, 103–107 (1732/33). This is available online from the The Euler Archive (in Latin unfortunately; accessed 2/26/2022). This leaves the mathematical community of the 18th century with the limited knowledge that the largest Fermat number which is prime is $F_4 = 65{,}537$. In fact, almost 300 years later we live with the same limited knowledge! The Wikipedia page on Fermat numbers (accessed 2/26/2022) lists the following unresolved questions about Fermat systems:

1. Is $F_n$ composite for all $n > 4$?
2. Are there infinitely many Fermat primes?
3. Are there infinitely many composite Fermat numbers?

**Note.** The next result explains why Fermat insisted on an exponent of 2 which is itself a power of 2.

**Theorem 6.66.** If $k \in \mathbb{N}$ and $n = 2^k + 1$ is prime, then $k$ is a power of 2.

**Note.** The next result, due to George Pólya (December 13, 1887–September 7, 1985), will allow us to show that any two Fermat numbers are relatively prime.

**Lemma 6.67.** For each $n \geq 1$, $F_n - 2 = F_0 F_1 \cdots F_{n-1}$.

**Definition.** A set $\{1_1, a_2, \ldots\}$ of integers is *pairwise relatively prime* if $(a_i, a_j) = 1$ for all $i \neq j$.

**Theorem 6.68.** The Fermat numbers are pairwise relatively prime.

**Note.** Notice that if there were only finitely many primes, then (by the Fundamental Theorem of Arithmetic, Theorem 6.29) we wouldn't have enough primes to make infinitely many pairwise relatively prime Fermat numbers. So we have a second argument that there are infinitely many primes (so we state Euclid's Theorem 6.16 again).

**Corollary 6.69.** There are infinitely many primes.

**Note.** We quickly introduce an application of calculus ideas to number theory. This vague idea is part of *analytic number theory*. One aspect of this is explored in complex analysis. See my online Complex Analysis (MATH 5510/5520) notes on Section VII.8. The Riemann Zeta Function; notice Euler's Theorem (Theorem VII.8.17) and the list of exercises following it. Leonhard Euler was the first to use analysis ideas in a number theory setting. He used series to prove that there are infinitely many prime numbers in his "Variae observations circa series infinitas," *Commentarii Academiae Scientiarum Petropolitanae*, **9** 160–188 (1737); this is available on the The Euler Archive (in Latin; accessed 2/27/2022).

**Note 6.7.A.** We recall three properties of series from Calculus 2 (MATH 1920).

1. Suppose $\{a_n\}_{n\geq 0}$ and $\{b_n\}_{n\geq 0}$ are sequences of nonnegative numbers. The *product* of the infinite series $\sum_{n=0}^{\infty} a_n$ and $\sum_{n=0}^{\infty} b_n$ is the series $\sum_{n=0}^{\infty} c_n$, where $c_n = \sum_{i=0}^{n} a_i b_{n-i}$. If the two given series converge to $L_1$ and $L_2$, then $\sum_{n=0}^{\infty} c_n$ converges with limit $L_1 L_2$. See my online Calculus 2 notes on Section 10.7. Power Series (notice Theorem 19, The Series Multiplication Theorem for Power Series).
2. If $0 < r < 1$, then $\displaystyle\sum_{n=0}^{\infty} r^n = \frac{1}{1-r}$. This is a *geometric series* with ratio $r$. See my Calculus 2 notes on Section 10.2. Infinite Series.
3. The series $1 + \dfrac{1}{2} + \dfrac{1}{3} + \dfrac{1}{4} + \cdots = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n}$ diverges. This is the *harmonic series*. See my Calculus 2 notes on Section 10.3. The Integral Test.
4. If $\sum_{n=0}^{\infty} |a_n|$ converses and $b_1, b_2, \ldots, b_n, \ldots$ is any rearrangement of the sequence $\{a_n\}_{n\geq 0}$ then $\sum_{n=0}^{\infty} |b_n|$ converges and $\sum_{n=0}^{\infty} b_n = \sum_{n=0}^{\infty} a_n$.See my Calculus 2 notes on Section 10.6. Alternating Series, Absolute and Conditional Convergence (notice Theorem 17, The Rearrangement Theorem for Absolutely Convergent Series).

We now have the equipment to give Euler's proof.

**Theorem 6.71.** There are infinitely many prime numbers.

**Note.** Notice that we now have three proofs that there are infinitely many prime numbers. We have Euclid's proof (Theorem 6.16), a proof based on Fermat numbers (Corollary 6.69), and Euler's proof using series.

*Revised: 2/27/2022*