Fermat and Mersenne Primes

The French monk Father **Marin Mersenne** (French theologian, philosopher and mathematician; 1588 - 1648) was an important facilitator of mathematical communication. He helped mathematics successfully escape from the Dark Ages that had stagnated intellectual life.

Pierre de Fermat (French lawyer and mathematician ; 1601 - 1665), whose monumental contributions to number theory are explored throughout most of the forthcoming chapters, frequently communicated with Mersenne.

In one letter to Mersenne Fermat announced he had "found that numbers of the form $2^{2^n} + 1$ are always prime numbers and have long since signified to the analysts the truth of this theorem."

In honor of Fermat, we call these numbers **Fermat numbers** and denote the general Fermat number by $F_n = 2^{2^n} + 1$

As Fermat observed,

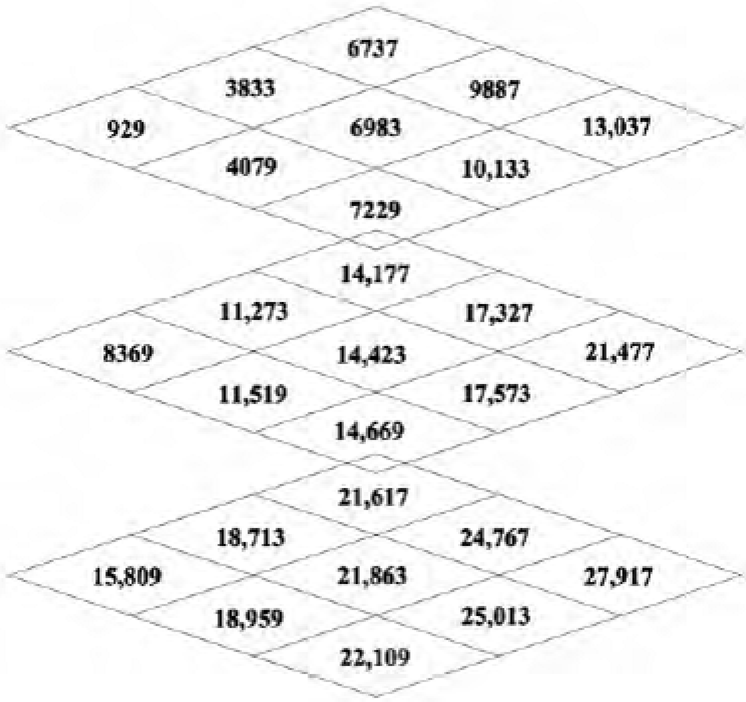
$$F_0 = 2^{2^0} + 1 = 3,$$

$$F_1 = 2^{2^1} + 1 = 5, \text{ and,}$$

$$F_2 = 2^{2^2} + 1 = 17$$

are all prime.

1. Determine F_3 by hand.



2. From the image above, you can see that F_3 is prime. Check this using only a basic calculator. Explain precisely how you have proven that this number is prime.

3. Using only a basic calculator, determine F_4.

4. Using a basic calculator, how long do you think it would take you to determine whether F_4 was prime? Explain.

5. To determine whether the fifth Fermat number, $F_5 = 2^{2^5} + 1 = 4{,}294{,}967{,}297$, is prime, theoretically what must one do?

6. In light of Fermat's virtually unblemished record, would it seem wise to challenge the primality of the fifth Fermat number in an era when computers and electronic calculators were not available?

Euler was the first to fruitfully extend any of Fermat's significant work in number theory. That is the case here as well.

Instead of using brute force to try to find factors of F_5, Euler ingeniously eliminated the majority of potential factors by analyzing properties potentially successful divisors would be required to have. In particular, he showed that if F_5 was not prime it must have a prime factor of the form $64k + 1$ where k is a positive integer.

7. Compute the numbers $64k + 1$ for $k = 1,2,...,10$.

8. Which of the ten numbers in your answer to Investigation **7** are prime?

9. Check to see if any of the primes from your answer to Investigation **8** divide F_5. What does this tell you about F_5?

When a Fermat number is prime we refer to it as a **Fermat prime**.

10. Would you be surprised to learn that mathematicians have shown that the next twenty six Fermat numbers, $F_6 = 2^{2^6} + 1$, ..., $F_{32} = 2^{2^{32}} + 1$are all composite? They are. How badly mistaken was Fermat in his conjecture about Fermat primes?

Mersenne Primes

In addition to his correspondence with Fermat, Mersenne made his own important contributions in the search for primes. He suggested that we consider numbers of the form

$$M_n = 2^n - 1,$$

numbers which have since been called **Mersenne numbers** in his honor. The first four Mersenne numbers are

$$M_2 = 2^2 - 1 = 3,$$
$$M_3 = 2^3 - 1 = 7, \text{and,}$$
$$M_4 = 2^4 - 1 = 15.$$

When Mersenne numbers are prime, like $M_2 = 3$ and $M_3 = 7$, they are called **Mersenne primes**.

11. Find the next six Mersenne numbers, $M_5 - M_{10}$.

12. Which of these Mersenne numbers are prime?

13. Based on the evidence you have thus far, can you make a conjecture - based on specific conditions on n - about when a Mersenne number M_n i) is a prime, and, ii) is not a prime? Explain.

14. What does your conjecture in Investigation **13** tell you about Mersenne numbers M_n when n is even and greater than 2? Explain.

15. Compute each of the products $(2^2 + 1) \cdot (2^2 - 1)$,$(2^3 + 1) \cdot (2^3 - 1)$, and $(2^4 + 1) \cdot (2^4 - 1)$. How do these products relate to Mersenne numbers?

16. Extend your observations in Investigation **15** to prove your conjecture in Investigation **14**.

17. The thirteenth, seventeenth, and nineteenth Mersenne numbers ($M_{13} = 2^{13} - 1 = 8191$,$M_{17} = 2^{17} - 1 = 131{,}071$, and $M_{19} = 2^{19} - 1 = 524{,}287$, respectively) are all prime numbers. Do these facts and your proof in Investigation **16** bolster your faith in the validity of your conjecture in Investigation **14** about the Mersenne numbers that are prime?

18. Is the eleventh Mersenne number, $M_{11} = 2^{11} - 1 = 2047$ prime? What does this tell you about your conjecture in Investigation **16**?