

1.1 A Prime Factory

WORKSHEET

The question

The n th Fermat number, F_n , is defined by

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, \dots,$$

where 2^{2^n} means 2 raised to the power 2^n .

Calculate F_0 , F_1 , F_2 and F_3 . Show that, for $k = 1$, $k = 2$ and $k = 3$,

$$F_0 F_1 \cdots F_{k-1} = F_k - 2. \quad (*)$$

Prove, by induction or otherwise, that $(*)$ holds for all $k \geq 1$. Deduce that no two Fermat numbers have a common factor greater than 1.

Hence show that there are infinitely many prime numbers.

Hints

Try the question on your own first. If you get stuck, read the hints *one at a time*, and go back to the question after each one. Hints marked *Pause and try* are the key steps.

- ? **Ask yourself** The last line asks about *infinitely many primes*. The middle asks about *common factors*. What could possibly connect “no two Fermat numbers share a factor” with “there are infinitely many primes”?

STAGE 1 Getting a feel for the numbers

- ? **Ask yourself** What do you notice about these four numbers?

STAGE 2 Checking the identity

- ? **Ask yourself** Look at the step from $k = 2$ to $k = 3$. We took 15, multiplied by 17, and got 255. In terms of Fermat numbers, we computed $(F_2 - 2) \times F_2$ and got $F_3 - 2$. Is that a coincidence?

STAGE 3 Proving the identity

Pause and try Before reading on, try to show directly that

✓
$$(F_k - 2) F_k = F_{k+1} - 2.$$

Hint: write everything in terms of powers of 2. What does $F_k - 2$ look like?

- ? **Ask yourself** This is a product of the form $(a - 1)(a + 1)$. What is that?

- ? **Ask yourself** What exactly do we need to show in the inductive step?

- ? **Ask yourself** Could we have avoided induction altogether?

STAGE 4 No common factors

- ? **Ask yourself** Suppose some number d divides both F_m and F_n , with $m < n$. Where does F_m appear in $(*)$?

- ? **Ask yourself** Now d divides F_n and $F_n - 2$. What else must it divide?

? **Ask yourself** Can d be 2?

STAGE 5 Infinitely many primes

? **Ask yourself** Every whole number greater than 1 has at least one prime factor. Pick one prime factor of each Fermat number. What can you say about the primes you have picked?

Try this next

- 1 **Euclid's version.** Write out Euclid's proof that there are infinitely many primes. In what sense is it "by contradiction", and in what sense is the Fermat-number proof "constructive"?
- 2 **The last digit.** Show that for $n \geq 2$ the Fermat number F_n ends in the digit 7.
- 3 **Sylvester's sequence.** Define $a_1 = 2$ and $a_{n+1} = a_n^2 - a_n + 1$, so the sequence begins 2, 3, 7, 43, 1807, ...
 - (a) Show that $a_{n+1} - 1 = a_1 a_2 \cdots a_n$.
 - (b) Deduce that the terms are pairwise coprime, and hence give another proof that there are infinitely many primes.
 - (c) **HARDER** Show that $\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} = 1 - \frac{1}{a_{n+1} - 1}$.
- 4 **Euler's trick.** *This needs Fermat's Little Theorem: if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.* Suppose a prime p divides F_n .
 - (a) Show that $2^{2^n} \equiv -1 \pmod{p}$, and hence that $2^{2^{n+1}} \equiv 1 \pmod{p}$.
 - (b) Let d be the smallest positive integer with $2^d \equiv 1 \pmod{p}$. Show that d divides 2^{n+1} but not 2^n , and conclude that $d = 2^{n+1}$.
 - (c) Using Fermat's Little Theorem, show that d divides $p - 1$. Deduce that $p \equiv 1 \pmod{2^{n+1}}$.
 - (d) For $n = 5$, this says any prime factor of F_5 has the form $64k + 1$. Check that 641 does. How many primes of this form are smaller than 641?
- 5 **A bound on the primes.** Use the argument in *One theorem, many proofs* to show that the n th prime is at most $2^{2^{n-1}} + 1$. How good is this bound when $n = 5$?

Further reading

- **Martin Aigner & Günter M. Ziegler, *Proofs from THE BOOK*** (Springer), Chapter 1, "Six proofs of the infinity of primes". It includes this proof alongside Euclid's and four

others, one of which uses topology. One of the best books you can read before university.

- ▶ **Harold Davenport, *The Higher Arithmetic*** (Cambridge University Press), Chapters 1–2. A beautifully written introduction to primes and factorisation, ideal for the summer before university.
- ▶ **Michal Křížek, Florian Luca & Lawrence Somer, *17 Lectures on Fermat Numbers*** (Springer, 2001). Everything about Fermat numbers, from Euler’s factorisation to Gauss’s polygons. Dip into the early chapters.
- ▶ **Ian Stewart, *Why Beauty Is Truth*** (Basic Books), the chapter on Gauss. The story of the 17-gon told for a general reader.

The full guided solution, and what the question leads to at university, is in Section 1.1:
https://keithmcnulty.github.io/step_book_mcnulty/ch01/fermat-numbers.html