FERMAT NUMBERS AND THEIR FACTORS

KEITH CONRAD

1. Introduction

A *Fermat number* is an integer of the form $F_n = 2^{2^n} + 1$, where $n \geq 0$. The first six Fermat numbers are

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \quad F_5 = 4294967297.$$

Fermat checked that F_n is prime for $n = 0, 1, 2, 3, 4$ and he conjectured that F_n is prime for all n. This was disproved when Euler [1] showed without explanation that $F_5 = 641 \cdot 6700417$, and in fact no further prime Fermat numbers have ever been found. Euler later explained how he factored F_5 [2, Thm. 8] (see also [6]): he proved for primes p that

$$p \mid F_n \Longrightarrow p \equiv 1 \bmod 2^{n+1}. \tag{1.1}$$

Thus prime factors of F_5 satisfy $p \equiv 1 \bmod 64$. The first such primes are $1 + 64k$ when $k = 3, 4, 7, 9$, and 10. At $k = 10$ we get $p = 1 + 64 \cdot 10 = 641$, so Euler's congruence condition on prime factors of Fermat numbers leads to a prime factor of F_5 in just five steps.

We will prove (1.1) by using the fact that the order of each nonzero number modulo p divides $p - 1$. Then, using the square patterns

$$2 \equiv \square \bmod p \iff p = 2 \text{ or } p \equiv 1, 7 \bmod 8,$$
$$3 \equiv \square \bmod p \iff p = 2, 3 \text{ or } p \equiv 1, 11 \bmod 12,$$

and Euler's criterion $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$, we will increase the modulus in (1.1) and derive a primality test for Fermat numbers.

2. Congruence conditions on prime factors of Fermat numbers

Theorem 2.1 (Euler)**.** *If a prime p divides $2^{2^n} + 1$ then $p \equiv 1 \bmod 2^{n+1}$.*

Proof. if $p \mid (2^{2^n} + 1)$ then $2^{2^n} \equiv -1 \bmod p$, so squaring both sides gives us $2^{2^{n+1}} \equiv 1 \bmod p$. Therefore $2 \bmod p$ has order dividing 2^{n+1}. Every proper factor of 2^{n+1} divides 2^n and $2^{2^n} \equiv -1 \not\equiv 1 \bmod p$, so the order of $2 \bmod p$ can't divide 2^n. Thus $2 \bmod p$ must have order 2^{n+1}. That implies $2^{n+1} \mid (p - 1)$, so $p \equiv 1 \bmod 2^{n+1}$. □

Taking $n = 1$ in Theorem 2.1, $2^2 + 1 = 5$ and $5 \equiv 1 \bmod 2^{n+1}$ while $5 \not\equiv 1 \bmod 2^{n+2}$, so it appears that the conclusion of Theorem 2.1 is sharp. However, this is not true. In the late 1800s, Lucas [3, pp. 280–281] improved Euler's congruence when $n \geq 2$.

Theorem 2.2 (Lucas)**.** *If a prime p divides $2^{2^n} + 1$ and $n \geq 2$ then $p \equiv 1 \bmod 2^{n+2}$.*

Proof. As in the proof of Theorem 2.1, we have $2^{2^n} \equiv -1 \bmod p$ and squaring gives us $2^{2^{n+1}} \equiv 1 \bmod p$. Since $p \equiv 1 \bmod 2^{n+1}$ by Theorem 2.1 and $n + 1 \geq 3$ when $n \geq 2$, we have $p \equiv 1 \bmod 8$. That implies by the square pattern for 2 that $2 \equiv \square \bmod p$.

Write $2 \equiv s^2 \bmod p$, so the condition $2^{2^n} \equiv -1 \bmod p$ implies $s^{2^{n+1}} \equiv -1 \bmod p$. The argument at this point will be similar to what we did in Theorem 2.1, starting from $2^{2^n} \equiv -1 \bmod p$, but replacing 2 with s and n with $n+1$.

Squaring both sides of $s^{2^{n+1}} \equiv -1 \bmod p$ we get

$$s^{2^{n+2}} \equiv 1 \bmod p.$$

Therefore the order of $s \bmod p$ is a factor of 2^{n+2}. If the order of $s \bmod p$ is not 2^{n+2} then it divides 2^{n+1}, so $s^{2^{n+1}} \equiv 1 \bmod p$, which is false. Thus $s \bmod p$ has order 2^{n+2}, so $2^{n+2} \mid (p-1)$, or $p \equiv 1 \bmod 2^{n+2}$. □

Example 2.3. Theorem 2.2 says prime factors of F_5 satisfy $p \equiv 1 \bmod 128$. The first such prime is $1 + 128 \cdot 2 = 257$ and the second is $1 + 128 \cdot 5 = 641$, so we are led to a prime factor of F_5 in two steps rather than five steps as we saw earlier. So if Euler had known Theorem 2.2 then he could have reduced his work to find the factor 641 of F_5.

Remark 2.4. For $5 \leq n \leq 12$ except $n = 8$, some prime factor of $2^{2^n} + 1$ is $1 \bmod 2^{n+2}$ but not $1 \bmod 2^{n+3}$, so perhaps Theorem 2.2 is sharp.

The reader can check as an exercise that Theorem 2.1 is true for odd prime factors of $a^{2^n} + 1$ no matter what integer a is: any odd prime p dividing such a number must satisfy $p \equiv 1 \bmod 2^{n+1}$. However, Theorem 2.2 does not generalize to other bases so easily. For example, the prime factors of $6^8 + 1$ are not congruent to $1 \bmod 2^{3+2}$ and two of the prime factors of $6^{16} + 1$ are not congruent to $1 \bmod 2^{4+2}$. Similarly, no prime factor of $10^4 + 1$ is $1 \bmod 2^{2+2}$ and no prime factor of $10^8 + 1$ is $1 \bmod 2^{3+2}$.

3. Determining primality of Fermat numbers

The following necessary and sufficient condition for primality of Fermat numbers has been used to prove (with computers) that some Fermat numbers are composite.

Theorem 3.1 (Pépin, 1877)**.** *For $n \geq 1$, F_n is prime if and only if $3^{(F_n-1)/2} \equiv -1 \bmod F_n$.*

Proof. First we show $F_n \equiv 5 \bmod 12$ for $n \geq 1$. (This is not true for $n = 0$ since $F_0 = 3$.) For $n \geq 1$, 2^n is even, so

$$F_n = 2^{2^n} + 1 = (-1)^{2^n} + 1 \equiv 2 \bmod 3.$$

Also $F_n \equiv 1 \bmod 4$ since $2^{2^n} \equiv 0 \bmod 4$ when $n \geq 1$. Combining these congruence conditions, $F_n \equiv 7 \bmod 12$ when $n \geq 1$.

($\Longrightarrow$) Suppose $p := F_n$ is prime. Since $p \equiv 5 \bmod 12$ we have $3 \not\equiv \square \bmod p$, so $3^{(p-1)/2} \equiv -1 \bmod p$ by Euler's criterion.

($\Longleftarrow$) Suppose $3^{(F_n-1)/2} \equiv -1 \bmod F_n$. We want to prove F_n is prime. Since $\frac{F_n-1}{2} = 2^{2^n-1}$, we have

$$3^{2^{2^n-1}} \equiv -1 \bmod F_n. \tag{3.1}$$

Squaring both sides,

$$3^{2^{2^n}} \equiv 1 \bmod F_n.$$

so the order of $3 \bmod F_n$ divides 2^{2^n}. If the order is not 2^{2^n}, then it is 2^e for some $e \leq 2^n - 1$. But $e \leq 2^n - 1 \Rightarrow 2^e \mid 2^{2^n-1}$, so $3^{2^{2^n}-1} \equiv 1 \bmod F_n$, which contradicts (3.1). Thus $3 \bmod F_n$ has order $2^{2^n} = F_n - 1$, so $(F_n - 1) \mid \varphi(F_n)$. Since $\varphi(m) \leq m - 1$ for all $m \geq 2$, from $(F_n - 1) \mid \varphi(F_n)$ we get $\varphi(F_n) = F_n - 1$. That means every nonzero integer mod F_n is a unit mod F_n, so F_n is a prime number. □

Remark 3.2. This proof can be adapted to a more general result: for an $n \geq 1$, if q is an odd prime such that $(\frac{F_n}{q}) = -1$, then F_n is prime if and only if $q^{(F_n-1)/2} \equiv -1 \bmod F_n$. To prove ($\Longleftarrow$) proceed exactly as in the case $q = 3$ (which is a choice of q for every $n \geq 1$ since $(\frac{F_n}{3}) = (\frac{2}{3}) = -1$). To prove ($\Longrightarrow$), that $F_n \equiv 1 \bmod 4$ when $n \geq 1$ lets us rewrite $(\frac{F_n}{q}) = -1$ as $(\frac{q}{F_n}) = -1$ by quadratic reciprocity and then use Euler's criterion.

Like Fermat's compositeness test (if $a^{m-1} \not\equiv 1 \bmod m$ for some a from 1 to $m-1$ then m is composite) when Pépin's theorem shows F_n is composite it does not yield a non-trivial factor of F_n. For instance, Pépin's theorem was used to prove F_{14} is composite in 1961, but a nontrivial factor of F_{14} was not found until almost 50 years later, in 2010.

A year after Pépin's work, Proth announced a result that is essentially a generalization.

Theorem 3.3 (Proth, 1878)**.** *Let $m = 2^k\ell + 1$, where ℓ is odd and $2^k > \ell$. The number m is prime if and only if there is an $a \in \mathbf{Z}$ such that $a^{(m-1)/2} \equiv -1 \bmod m$.*

A Fermat number $2^{2^n} + 1$ is $2^k\ell + 1$ for $k = 2^n$ and $\ell = 1$. Pépin's theorem is slightly stronger than Proth's theorem in this case because Pépin says we can definitely use $a = 3$, so Proth's theorem is not strictly speaking a generalization of Pépin's theorem.

Proof. If m is prime then $a^{(m-1)/2} \equiv -1 \bmod m$ when $a \not\equiv \square \bmod m$ and half the nonzero integers mod m satisfy this condition.

Conversely, assume some integer a satisfies $a^{(m-1)/2} \equiv -1 \bmod m$. We will prove m is prime by an argument based on [5]. The congruence $a^{(m-1)/2} \equiv -1 \bmod m$ is the same $a^{2^{k-1}\ell} \equiv -1 \bmod m$. Let p be a prime factor of m, so

$$a^{2^{k-1}\ell} \equiv -1 \bmod p. \tag{3.2}$$

Squaring both sides, we get $a^{2^k\ell} \equiv 1 \bmod p$. Therefore the order of $a \bmod p$ divides $2^k\ell$, so it has the form $2^e\ell'$, where $e \leq k$ and ℓ' is a factor of ℓ. If $e < k$ then $2^e\ell' \mid 2^{k-1}\ell$, so $a^{2^{k-1}\ell} \equiv 1 \bmod p$. That contradicts (3.2), so $e = k$: $a \bmod p$ has order $2^k\ell'$ where $\ell' \mid \ell$. Therefore $2^k\ell' \mid (p-1)$, so $2^k \mid (p-1)$. This implies $2^k \leq p-1$, so $p > 2^k$.

We showed every prime factor of m is greater than 2^k. Therefore if m is not prime, so it is a product of more than one prime, we have $m > 2^{2k}$. However, by the hypotheses of the theorem we have $m = 2^k\ell + 1 \leq 2^k(2^k - 1) + 1 = 2^{2k} - 2^k + 1 < 2^{2k}$, which is a contradiction. □

Example 3.4. Let $m = 31489$. Then $m - 1 = 31488 = 2^8 \cdot 123$ and $2^8 = 256 > 123$. We have $a^{(m-1)/2} \equiv 1 \bmod m$ for $a = 2$, 3, and 5, but $7^{(m-1)/2} \equiv -1 \bmod m$, so m is prime by Proth's theorem using $a = 7$.

Proth's theorem at first sight seems incredible: it lets us *prove* primality of m by verifying a congruence condition mod m for a single well-chosen a that should exist in great abundance if m really is prime. The catch is that m has to have a special form to apply Proth's theorem: m needs to be odd with the highest power of 2 dividing $m - 1$ being greater than the odd part of $m - 1$. This is *not typical* of most odd numbers, or even most odd prime numbers.

References

[1] L. Euler, "Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus," *Novi Commentarii Academiae Scientiarum Petropolitana* **6** (1732/33) 1738, 103–107. URL http://eulerarchive.maa.org/pages/E026.html.

[2] L. Euler, "Theoremata circa divisors numerorum," *Novi Commentarii Academiae Scientiarum Petropolitanae* **1** (1747/48) 1750, pp. 20–48. URL http://eulerarchive.maa.org/pages/E134.html.
[3] É. Lucas, "Théorèmes d'arithmétique," *Atti della Reale Accademia delle Scienze di Torino* **13** (1878), 271–284.
[4] F. Proth, "Théorèmes sur les nombres premiers," *C. R. Acad. Sci. Paris* **87** (1878) 926.
[5] R. Robinson, "The converse of Fermat's theorem," *Amer. Math. Monthly* **64** (1957), 703–710.
[6] E. Sandifer, "How Euler did it: factoring F_5," 2007. URL http://eulerarchive.maa.org/hedi/HEDI-2007-03.pdf.