A primality test for Fermat numbers

A. GRYTCZUK and J. GRYTCZUK

Abstract. Relying on some properties of Bernoulli numbers we derive a new primality criterion for Fermat numbers $F_n=2^{2^n}+1$.

1. Introduction. For a given a sequence of positive integers it is often very hard to decide whether there are infinitely many primes among its terms. Consider for example the sequence $2+1,\ 2^2+1,\ 2^3+1, 2^4+1, \ldots$. It is an easy observation that $2^m+1, m>0$ can be a prime only if m is itself a power of 2. So, we obtain in this way the Fermat numbers $F_n = 2^{2^n}+1, n \geq 0$. The first five of them are $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257,\ F_4 = 65\,537$ and they are all primes. Fermat thought that this pattern persists but Euler found that F_5 is composite: $F_5 = 2^{32}+1 = (641)(6700417)$. In fact, for $4 < n < 24$ and for many larger values of of n Fermat numbers are known to be composite. It is strange that beyond F_5 no further Fermat primes have been found.

The prupose of this note is to give a necessry and sufficient condition for the Fermat number F_n to be a prime. Our test is similar to the Lucas—Lehmer test for Mersenne numbers $M_n = 2^n - 1$ (see [2]). Indeed, primality of F_n depends on whether F_n divides an appropriate term of the recurrent sequence $T(m)$ defined by

$$\text{(1a)} \quad T(1) = 1,$$

$$\text{(1b)} \quad T(m) = (-1)^{m-1} + \sum_{i=1}^{m-1} (-1)^{i+1} \binom{2m-1}{2i} T(m-i), \quad m > 1.$$

This is stated in the following theorem.

Theorem. Let k and n be fixed positive integers such that $0 < k \leq [\log n \log 2]$, $n > 1$ and let $T(m)$ be as above. Then the Fermat number F_k is a prime if and only if F_k does not divide $T(2^{n-1})$.

2. Proof of the Theorem. We derive our assertion from the following lemma.

Lemma. Let B_{2m} denote the $2m$-th Bernoulli number. Then for every

positive integer m we have

$$B_{2m} = (-1)^{m-1} m T(m) \Big/ 2^{2m-1}(2^{2m} - 1) \tag{2}$$

where $T(m)$ is defined by (1a) and (1b).

Proof. It is well known (see e.g. [1]) that

$$B_{2m} = (-1)^{m-1} m T_m \Big/ 2^{2m+1}(2^{2m} - 1)$$

where T_m are coefficients in the power series expansion of the function $\operatorname{tg} x$, i. e.

$$\operatorname{tg} x = \sum_{m=1}^{\infty} T_m \frac{x^{2m-1}}{(2m-1)!}.$$

Thus, we are going to prove that $T(m) = T_m$ for all $m > 0$. In fact, we can write

$$\sum_{m=1}^{\infty} T_m \frac{x^{2m-1}}{(2m-1)!} \sum_{m=0}^{\infty} (-1)^m \frac{x^{2m}}{(2m)!} = \sum_{m=1}^{\infty} (-1)^{m-1} \frac{x^{2m-1}}{(2m-1)!}. \tag{3}$$

By comparing coefficients of x^{2m-1} we have $T_1 = 1$ and

$$\begin{aligned} T_m \Big/ (2m-1)! - T_{m-1} \Big/ 2!(2m-3)! + \\ + T_{m-2} \Big/ 4!(2m-5)! - \cdots = (-1)^{m-1} \Big/ (2m-1)!. \end{aligned} \tag{4}$$

Hence

$$T_m - \binom{2m-1}{2} T_{m-1} + \binom{2m-1}{4} T_{m-2} - \cdots = (-1)^{m-1}$$

and the proof of Lemma is complete.

For the proof of the Theorem put $m = 2^{n-1}$. Then we have

$$B_{2^n} = \frac{(-1)2^{n-1} T(2^{n-1})}{2^{2^n-1}(2^{2^n} - 1)} = \frac{(-1)2^{n-1} T(2^{n-1})}{2^{2^n-1} F_0 F_1 \cdots F_{n-1}}. \tag{5}$$

But from the well known theorem of von Staudt and Clausen if follows that if we write $B_{2m} = N_{2m} \Big/ D_{2m}$ with $(N_{2m}, D_{2m}) = 1$ then

$$D_{2m} = \prod_{p-1 \mid 2m} p, \quad p \text{ prime}.$$

It is now easy to see that D_{2^n} is a product of 2 and Fermat primes F_k with k not greater then $\log n / \log 2$. This finishes the proof of Theorem.

References

[1] Z. I. BOREVICH and I. R. SHAFAREVICH, Number Theory, Moskva, 1964, (in Russian)

[2] P. RIBENBOIM, The Book of Prime Number Records, *Springer-Verlag*, 1988.