Journal of Integer Sequences, Vol. 28 (2025),
Article 25.8.7

Fermat Numbers Modulo a Prime

Jiří Klaška
Institute of Mathematics
Faculty of Mechanical Engineering
Brno University of Technology
Technická 2
CZ – 616 69 Brno
Czech Republic
klaska@fme.vutbr.cz

Abstract

Nearly forty years ago Aigner published an interesting theorem regarding the periodicity of the sequence of Fermat numbers reduced by a given prime modulus. In this article we perform a detailed analysis of Aigner's result and his proof. Above all, however, we show that Aigner's theorem can be substantially simplified and also refined.

1 Introduction

Let $F_n = 2^{2^n} + 1$ where $n \in \mathbb{N} \cup \{0\}$. The numbers F_n are called Fermat numbers after the French mathematician Pierre de Fermat (1601–1665). Many remarkable properties of Fermat numbers are known. See, for example, the books [3, 4] or consult The On-Line Encyclopedia of Integer Sequences [7, A000215].

In 1986, Austrian mathematician Alexander Aigner (1909–1988) published his final paper [1] in which he opened up a new issue of so-called elite primes. Recall that a prime p is called elite if only a finite number of Fermat numbers F_n are quadratic residues modulo p. See also [7, A102742].

Aigner's paper [1, p. 87] also contains an interesting theorem concerning the periodicity of the sequence $(F_n \bmod p)_{n=0}^{\infty}$, where p is a prime. Recall now the original German formulation of Aigner's theorem and his proof arguments.

Theorem 1. (Aigner, 1986) *Ist $p-1 = 2^r u$ mit ungeradem u und $2^s t$ mit $0 \le s \le r$ und $t \mid u$ der genaue "Potenzindex" des Restes $2 \bmod p$, so hat die Vorperiode $r-s$ Glieder und die Länge der Periode wird gleich der Ordnung h des Restes 2 in der multiplikativen Gruppe $\bmod\ u/t = u'$.*

Proof. Es existiert eine geeignete Primitivwurzel $g \bmod p$, so daß $2 \equiv g^{2^s t}$ ist. Quadrierung der Potenz mod p bedeutet Verdopplung des Exponenten mod $p-1$. Wir sind solange in der Vorperiode, als im Exponenten der Faktor 2^r noch nicht erreicht ist. Hernach sind alle Exponenten durch $2^r t$ teilbar. Und soll nach h Schritten die erste Wiederholung auftreten, so ergibt dies $2^{r+h} t \equiv 2^r t$ nach dem Modul $p-1 = 2^r t u'$ oder $2^h \equiv 1(u')$. ☐

Unfortunately, Aigner's result presented in Theorem 1 has not received the attention that it deserves and has not appeared in any of the recently published books [3, 4] specifically devoted to Fermat numbers. The main reason is probably that the paper [1] was published in German, which, along with some vague wording, makes it difficult to properly understand Theorem 1 and its proof. In this article, we carry out a detailed analysis of Aigner's result to show that Theorem 1 can be substantially simplified and also refined. The exact formulation of Theorem 1 and its proof in English is presented in Theorem 15 with its simplification provided by Theorem 20.

Throughout this paper, we adopt the following notation. If A is a finite set, $\#A$ denotes the number of elements of A. Specifically, if $A = \emptyset$, then $\#A = 0$.

2 Basic concepts and auxiliary results

We recall some of the basic definitions and known statements that we need later in the paper.

Lemma 2. *Let p be a prime. Then there exist $i, j \in \{0, 1, \ldots, p\}$ such that $i < j$ and $F_i \equiv F_j \pmod{p}$.*

Proof. The conclusion follows from Dirichlet's well-known pigeonhole principle. ☐

Remark 3. The reader may find some interesting facts on the history of this principle in article [5].

Lemma 4. *Let $i \in \mathbb{N} \cup \{0\}$, $j \in \mathbb{N}$ and let $i < j$. Further, let p be a prime. Then* (i) *and* (ii) *hold.*

(i) *If $F_i \equiv F_j \pmod{p}$, then $F_{i+t} \equiv F_{j+t} \pmod{p}$ for all $t \in \mathbb{N}$.*

(ii) *If $F_j \not\equiv F_{j+t} \pmod{p}$ for all $t \in \mathbb{N}$, then $F_i \not\equiv F_{i+t} \pmod{p}$ for all $t \in \mathbb{N}$.*

Proof. We prove (i). Let $t \in \mathbb{N}$. First, observe that

$$F_i \equiv F_j \pmod{p} \Longleftrightarrow 2^{2^i} \equiv 2^{2^j} \pmod{p}.$$

Next, by raising both sides of $2^{2^i} \equiv 2^{2^j} \pmod{p}$ to 2^t-th power we obtain $2^{2^{i+t}} \equiv 2^{2^{j+t}} \pmod{p}$. Hence, $F_{i+t} \equiv F_{j+t} \pmod{p}$.

We prove (ii). Suppose that $F_i \equiv F_{i+s} \pmod{p}$ for an $s \in \mathbb{N}$. Since $i < j$, there exists a $l \in \mathbb{N}$ such that $j = i + l$. Using part (i) of Lemma 2.3, we now get

$$F_j = F_{i+l} \equiv F_{i+l+s} = F_{j+s} \pmod{p},$$

which is a contradiction. □

It is clear, that Lemma 4 has a crucial importance for further considerations. Indeed, it guarantees that the sequence $(F_n \bmod p)_{n=0}^{\infty}$ becomes periodic at some point. In the usual terminology (see, for example, [7]) we say that $(F_n \bmod p)_{n=0}^{\infty}$ is an eventually (or ultimately) periodic sequence. Let us now recall some basic definitions.

Definition 5. Let p be a prime.

(i) Let $H(p) = \{h \in \mathbb{N} \cup \{0\} : F_h \not\equiv F_{h+i} \pmod{p} \text{ for all } i \in \mathbb{N}\}$ and let $h(p) = \#H(p)$. Then we call $h(p)$ *the length of the pre-period* of the sequence $(F_n \bmod p)_{n=0}^{\infty}$. Specifically, if $h(p) = 0$, then we say that $(F_n \bmod p)_{n=0}^{\infty}$ does not have a pre-period.

(ii) Let $i \in \mathbb{N} \cup \{0\}$, $j \in \mathbb{N}$ and let $i < j$. If $F_i \equiv F_j \pmod{p}$, we call the number $j - i$ *the length of the period* of $(F_n \bmod p)_{n=0}^{\infty}$.

(iii) Let $h(p)$ be the length of the pre-period of $(F_n \bmod p)_{n=0}^{\infty}$. Then we call the number $k(p) = \min\{t \in \mathbb{N} : F_{h(p)} \equiv F_{h(p)+t} \pmod{p}\}$ *the length of the primitive period* of the sequence $(F_n \bmod p)_{n=0}^{\infty}$.

An important relationship between the length of a period and the length of the primitive period $k(p)$ is provided by Lemma 6.

Lemma 6. *Let $i \in \mathbb{N} \cup \{0\}$, $j \in \mathbb{N}$ and let $i < j$. Further, let p be a prime. Then $F_i \equiv F_j \pmod{p}$ if and only if $i \geq h(p)$ and $i \equiv j \pmod{k(p)}$.*

Proof. Let $F_i \equiv F_j \pmod{p}$. Then, by Definition 5, $i \geq h(p)$ and $k(p) \leq j - i$. It is obvious that $j - i$ can be written uniquely in the form of $j - i = \alpha \cdot k(p) + \beta$ where $\alpha \in \mathbb{N}$, $\beta \in \mathbb{N} \cup \{0\}$ and $0 \leq \beta < k(p)$. Hence,

$$F_i \equiv F_j \pmod{p} \Longleftrightarrow F_i \equiv F_{i+\alpha \cdot k(p)+\beta} \pmod{p}. \tag{1}$$

On the other hand, we have $F_i \equiv F_{i+k(p)} \pmod{p}$ and, by induction, we find that $F_i \equiv F_{i+s \cdot k(p)} \pmod{p}$ for each $s \in \mathbb{N}$. In particular, if $s = \alpha$, then

$$F_i \equiv F_{i+\alpha \cdot k(p)} \pmod{p}. \tag{2}$$

Combining (1) and (2), we now get

$$F_{i+\alpha\cdot k(p)} \equiv F_{i+\alpha\cdot k(p)+\beta} \pmod{p}. \tag{3}$$

Suppose that $\beta \neq 0$. Then, by (3), $(F_n \bmod p)_{n=0}^{\infty}$ is periodic with the length of period equal to β. Since $\beta < k(p)$, we have a contradiction. Consequently, $\beta = 0$ and $j - i = \alpha \cdot k(p)$. Hence, $k(p) \mid j - i$, and $i \equiv j \pmod{k(p)}$ follows.

Let $i \geq h(p)$ and let $i \equiv j \pmod{k(p)}$. Then $k(p) \mid j - i$ and thus, there exists an $\alpha \in \mathbb{N}$ such that $j - i = \alpha \cdot k(p)$. This, together with $F_i \equiv F_{i+\alpha\cdot k(p)} \pmod{p}$, yields $F_i \equiv F_j \pmod{p}$, as required. □

It is also useful to recall the following definitions.

Definition 7. Let $a, m \in \mathbb{N}$ and let $\gcd(a, m) = 1$.

(i) The least $t \in \mathbb{N}$ such that $a^t \equiv 1 \pmod{m}$ is called the *multiplicative order* of a modulo m and is denoted by $\mathrm{ord}_m(a)$.

(ii) If $\mathrm{ord}_m(a) = \phi(m)$, then a is called a *primitive root* of m. Here, ϕ means the Euler function.

(iii) Let g be a primitive root of m. The unique $t \in \mathbb{N}$ satisfying $1 \leq t \leq \phi(m)$ and $g^t \equiv a \pmod{m}$ is called *index* (or *discrete logarithm*) of a to the base g modulo m and denoted by $\mathrm{ind}_g(a)$.

For the theory of indices and primitive roots, see, for example, [2, pp. 147–168] or [6, pp. 347–385].

Lemma 8. *Let $a, m, s, t \in \mathbb{N}$ and let $\gcd(a, m) = 1$. Then* (i)–(iv) *hold.*

(i) *$a^s \equiv 1 \pmod{m}$ if and only if $\mathrm{ord}_m(a) \mid s$. In particular, if $m = p$ is a prime, then $\mathrm{ord}_p(a) \mid p - 1$.*

(ii) *$a^s \equiv a^t \pmod{m}$ if and only if $s \equiv t \pmod{\mathrm{ord}_m(a)}$.*

(iii) *We have*

$$\mathrm{ord}_m(a^s) = \frac{\mathrm{ord}_m(a)}{\gcd(s, \mathrm{ord}_m(a))}.$$

(iv) *Let g be a primitive root of a prime p and let $a \in \{1, \ldots, p-1\}$. Then we have*

$$\gcd(p - 1, \mathrm{ind}_g(a)) = \frac{p-1}{\mathrm{ord}_p(a)}.$$

For a proof of part (i) of Lemma 8, see, for example, [2, p. 148] or [6, p. 348]. A proof of part (ii) can be found in [2, p. 148] or [6, p. 349]. For a proof of part (iii), see [2, p. 149] or [6, p. 351]. Finally, a proof of (iv) can be found in [8, p. 115].

3 Aigner's theorem revised

In this section, we use the following special case of the Chinese remainder theorem.

Theorem 9. *Let m_1 and m_2 be relatively prime positive integers. Then, for all integers a and b, the system of congruences*

$$x \equiv a \pmod{m_1}, \ x \equiv b \pmod{m_2}$$

has a solution, and this solution is uniquely determined modulo $m_1 m_2$.

For a proof of the Chinese remainder theorem see, for example [2, p. 79], or consult [6, p. 162].

Lemma 10. *Let $\alpha, \beta \in \mathbb{N}$ and let $\gcd(\alpha, \beta) = 1$. Then, for every $\gamma \in \mathbb{N}$, there exists a $c \in \mathbb{N}$ satisfying the conditions*

$$\gcd(c, \gamma) = 1, \ c \equiv \beta \pmod{\alpha}. \tag{4}$$

Proof. Let γ be a positive integer and let

$$d = \max\{\delta \in \mathbb{N} : \delta \mid \gamma, \ \gcd(\delta, \alpha) = 1\}. \tag{5}$$

The basic idea of the proof is as follows. We show that (4) is met by every solution $c \in \mathbb{N}$ of the system of congruences

$$c \equiv 1 \pmod{d}, \ c \equiv \beta \pmod{\alpha}. \tag{6}$$

First, observe that (7) immediately follows from (5).

$$\text{If } p \text{ is a prime satisfying } p \mid \frac{\gamma}{d}, \text{ then } p \mid \alpha. \tag{7}$$

Next, it is obvious that implication (8) applies.

$$\text{If } c \in \mathbb{N}, p \text{ is a prime satisfying } p \mid d \text{ and } c \equiv 1 \pmod{d}, \text{ then } p \nmid c. \tag{8}$$

Assume now that $c \in \mathbb{N}$, p is a prime satisfying $p \mid (\gamma/d)$ and that $c \equiv \beta \pmod{\alpha}$. Then, by (7), $p \mid \alpha$. Therefore there exists a $q \in \mathbb{N}$ such that $\alpha = pq$. Hence, $c \equiv \beta \pmod{pq}$, which implies $c \equiv \beta \pmod{p}$. Using the hypothesis $\gcd(\alpha, \beta) = 1$ we obtain $\gcd(pq, \beta) = 1$, and $\beta \not\equiv 0 \pmod{p}$ follows. This together with $c \equiv \beta \pmod{\alpha}$ yields $c \not\equiv 0 \pmod{p}$. Hence, (9).

$$\text{If } c \in \mathbb{N}, p \text{ is a prime satisfying } p \mid \frac{\gamma}{d}, \text{ and } c \equiv \beta \pmod{\alpha}, \text{ then } p \nmid c. \tag{9}$$

Combining (8) with (9) we see that, if $c \in \mathbb{N}$, p is a prime satisfying $p \mid \gamma = d \cdot (\gamma/d)$, $c \equiv 1 \pmod{d}$ and $c \equiv \beta \pmod{\alpha}$, then $p \nmid c$. Consequently, every solution $c \in \mathbb{N}$ of the system of congruences (6) satisfies (4).

Since, by (5), $\gcd(d, \alpha) = 1$, the system of congruences (6) is solvable by Theorem 9. Moreover, if c satisfies (6), then c is uniquely determined modulo αd. The proof is complete. ∎

Proposition 11. *Let p be a prime and let $a \in \{1, \dots, p-1\}$. Then there exists a primitive root g of p satisfying*

$$\operatorname{ind}_g(a) = \frac{p-1}{\operatorname{ord}_p(a)}. \tag{10}$$

Proof. Let h be a primitive root of p. Then there exists a unique $s \in \mathbb{N}$, $1 \le s \le \phi(p) = p-1$ such that $a \equiv h^s \pmod{p}$, that is, $s = \operatorname{ind}_h(a)$. Next, let t be positive integer satisfying $a^t \equiv 1 \pmod{p}$. From the assumptions made, it follows that

$$a^t \equiv 1 \pmod{p} \Longleftrightarrow h^{st} \equiv 1 \pmod{p} \Longleftrightarrow p-1 \mid st. \tag{11}$$

Let us now put $d := \gcd(p-1, s)$. Then we have

$$p-1 \mid st \Longleftrightarrow \frac{p-1}{d} \mid \frac{ts}{d} \Longleftrightarrow \frac{p-1}{d} \mid t. \tag{12}$$

Combining (11) with (12), we obtain

$$a^t \equiv 1 \pmod{p} \Longleftrightarrow \frac{p-1}{d} \mid t,$$

which means that

$$\operatorname{ord}_p(a) = \frac{p-1}{d}.$$

We now use Lemma 10. Let us put $\alpha := (p-1)/d$ and $\beta := s/d$. Since $\gcd(\alpha, \beta) = 1$, for each $\gamma \in \mathbb{N}$ there exists a $c \in \mathbb{N}$ satisfying (4). In particular for $\gamma = p-1$, there exists a $c \in \mathbb{N}$ such that

$$\gcd(c, p-1) = 1, \ c \equiv \frac{s}{d} \left(\operatorname{mod} \frac{p-1}{d}\right) \tag{13}$$

and this c is uniquely determined modulo $\alpha d = p-1$.

From the second relation of (13) we receive $cd \equiv s \pmod{p-1}$. Since h is a primitive root of p, we have $\operatorname{ord}_p(h) = p-1$, thus, $cd \equiv s \pmod{\operatorname{ord}_p(h)}$. Next, applying part (ii) of Lemma 8, we get

$$cd \equiv s \pmod{\operatorname{ord}_p(h)} \Longleftrightarrow h^{cd} \equiv h^s \pmod{p} \Longleftrightarrow h^{cd} \equiv a \pmod{p}. \tag{14}$$

Let us now prove that $g := h^c$ is a primitive root of p. Using part (iii) of Lemma 8 and applying the first part of (13), we obtain (15).

$$\operatorname{ord}_p(g) = \operatorname{ord}_p(h^c) = \frac{\operatorname{ord}_p(h)}{\gcd(c, \operatorname{ord}_p(h))} = \frac{p-1}{\gcd(c, p-1)} = p-1. \tag{15}$$

Finally, from $g \equiv h^c \pmod{p}$ it follows $g^d \equiv h^{cd} \pmod{p}$ and, by (14), we have $h^{cd} \equiv a \pmod{p}$. Hence, $g^d \equiv a \pmod{p}$. This together with $d = (p-1)/\operatorname{ord}_p(a)$ yields $\operatorname{ind}_g(a) = (p-1)/\operatorname{ord}_p(a)$, as required. $\square$

Remark 12. A primitive root g of a prime p satisfying (10) may not be determined uniquely. For example, if $a = 2$ and $p = 31$, then $\mathrm{ord}_{31}(2) = 5$. By direct calculation, we can find that there exist exactly two primitive roots of 31 satisfying (10)—namely, $\mathrm{ind}_{12}(2) = \mathrm{ind}_{21}(2) = 30/5 = 6$.

Proposition 13. *Let p be a prime and let $a \in \{1, \ldots, p-1\}$. Further, let g be a primitive root of p. Then we have*

$$\mathrm{ind}_g(a) \mid p-1 \text{ if and only if } \mathrm{ind}_g(a) = \frac{p-1}{\mathrm{ord}_p(a)}. \tag{16}$$

Proof. Let $\mathrm{ind}_g(a) \mid p-1$. Then there is a $c \in \mathbb{N}$ such that $p - 1 = c \cdot \mathrm{ind}_g(a)$. Hence,

$$\gcd(p-1, \mathrm{ind}_g(a)) = \mathrm{ind}_g(a) \cdot \gcd(c, 1) = \mathrm{ind}_g(a). \tag{17}$$

On the other hand, by part (iv) of Lemma 8, we have

$$\gcd(p-1, \mathrm{ind}_g(a)) = \frac{p-1}{\mathrm{ord}_p(a)}.$$

This, together with (17), yields $\mathrm{ind}_g(a) = (p-1)/\,\mathrm{ord}_p(a)$.

Since the converse implication is evident, the desired result follows. □

Corollary 14. *Let p be an odd prime and let $p - 1 = 2^r u$ where $r, u \in \mathbb{N}$ and $2 \nmid u$. Then there exist a uniquely determined $s \in \mathbb{N} \cup \{0\}$ and $t \in \mathbb{N}$ such that*

$$0 \le s \le r,\ \ t \mid u \text{ and } 2^s t = \mathrm{ind}_g(2) \text{ for some primitive root } g \text{ of } p. \tag{18}$$

Proof. First, by part (i) of Lemma 8, we have $\mathrm{ord}_p(2) \mid p - 1 = 2^r u$. This means that $\mathrm{ord}_p(2) = 2^q v$ for a $q \in \mathbb{N} \cup \{0\}$, $0 \le q \le r$ and $v \in \mathbb{N}$ satisfying $v \mid u$, $2 \nmid v$. Let us now put $s := r - q$ and $t := u/v$. Then $s \in \mathbb{N} \cup \{0\}$, $0 \le s \le r$, $t \in \mathbb{N}$, and $t \mid u$. Next, by Proposition 11, there exists at least one primitive root g of p such that

$$\mathrm{ind}_g(2) = \frac{p-1}{\mathrm{ord}_p(2)} = \frac{2^r u}{2^q v} = 2^s t.$$

From this and from (16) it now follows that s and t are the only numbers satisfying (18). □

We are now ready to properly understand Aigner's Theorem 1, presented in the introduction. Theorem 1 can be formulated more exactly as follows.

Theorem 15. *Let p be an odd prime and let $p - 1 = 2^r u$ where $r, u \in \mathbb{N}$ and $2 \nmid u$. Then* (i)–(iii) *hold.*

(i) *There exist uniquely determined $s \in \mathbb{N} \cup \{0\}$ and $t \in \mathbb{N}$ such that $0 \le s \le r$, $t \mid u$ and $2^s t = \mathrm{ind}_g(2)$ for some primitive root g of p.*

(ii) $h(p) = r - s$.

(iii) $k(p) = \mathrm{ord}_{u'}(2)$, *where* $u' = u/t$.

Proof. Since the proof of (i) has already been given in Corollary 14, it is sufficient to prove (ii) and (iii).

We prove (ii). Let g be a primitive root of p and let $\mathrm{ind}_g(2) = 2^s t$ where $s \in \mathbb{N} \cup \{0\}$, $0 \le s \le r$, $t \in \mathbb{N}$, and $t \mid u$. Then by part (i) of Theorem 15, s and t are uniquely determined and we have

$$2 \equiv g^{2^s t} \pmod{p}. \tag{19}$$

By raising both sides of (19) to 2^j, with $j \in \mathbb{N} \cup \{0\}$, we obtain

$$2^{2^j} \equiv g^{2^{s+j} t} \pmod{p}. \tag{20}$$

Let $w \in \mathbb{N} \cup \{0\}$ and let $0 \le w < r - s$. Suppose that $F_w \equiv F_{r-s} \pmod{p}$. Then we have

$$2^{2^w} \equiv 2^{2^{r-s}} \pmod{p}. \tag{21}$$

We now use (20). Taking $j = w$, we obtain $2^{2^w} \equiv g^{2^{s+w} t} \pmod{p}$ and, taking $j = r - s$, we get $2^{2^{r-s}} \equiv g^{2^r t} \pmod{p}$. The last two congruences together with (21) lead to

$$g^{2^{s+w} t} \equiv g^{2^r t} \pmod{p}. \tag{22}$$

Because g is a primitive root of p, we have $\mathrm{ord}_p(g) = p - 1$. Applying part (ii) of Lemma 8, we now see that (22) is equivalent to

$$2^{w+s} t \equiv 2^r t \pmod{p-1}. \tag{23}$$

Furthermore, $t \mid u$ implies that there exists a $u' \in \mathbb{N}$ such that $u = tu'$. This means that $p - 1 = 2^r tu'$. Since $w < r - s$, there exists an $l \in \mathbb{N}$ such that $w + l = r - s$. Substituting $r = s + w + l$ and $p - 1 = 2^{s+w+l} tu'$ into (23), we obtain

$$2^{w+s} t \equiv 2^{s+w+l} t \pmod{2^{s+w+l} tu'}. \tag{24}$$

From (24) now it follows that $2^l \equiv 1 \pmod{2^l u'}$, which yields $2^l \mid 2^l - 1$, a contradiction. Consequently, $F_w \not\equiv F_{r-s} \pmod{p}$ for every $w \in \{0, \ldots, r - s - 1\}$. Therefore,

$$h(p) \ge \#\{0, \ldots, r - s - 1\} = r - s. \tag{25}$$

Now we show that there exists an $l \in \mathbb{N}$ such that

$$F_{r-s} \equiv F_{r-s+l} \pmod{p}, \ \text{or equivalently,} \ 2^{2^{r-s}} \equiv 2^{2^{r-s+l}} \pmod{p}. \tag{26}$$

Again, applying (20), for $j = r - s$ we obtain $2^{2^{r-s}} \equiv g^{2^r t} \pmod{p}$ and, for $j = r - s + l$, we get $2^{2^{r-s+l}} \equiv g^{2^{r+l}t} \pmod{p}$. Combining the last two congruences with (26) we get $g^{2^r t} \equiv g^{2^{r+l}t} \pmod{p}$, which is, by part (ii) of Lemma 8, equivalent to $2^r t \equiv 2^{r+l} t \pmod{p-1}$. Because $p - 1 = 2^r t u'$, it is clear that $2^l \equiv 1 \pmod{u'}$ and, by part (i) of Lemma 8, we conclude that $2^l \equiv 1 \pmod{u'}$ holds for every $l = c \cdot \operatorname{ord}_{u'}(2)$ where $c \in \mathbb{N}$. From (26) now it follows that $h(p) \leq r - s$, which together with (25) proves (ii).

We prove (iii). First, taking $l = \operatorname{ord}_{u'}(2)$ in (26), we obtain

$$F_{r-s} \equiv F_{r-s+\operatorname{ord}_{u'}(2)} \pmod{p},$$

which means that $\operatorname{ord}_{u'}(2)$ is the length of a period of $(F_n \bmod p)_{n=0}^{\infty}$. Applying Lemma 6, we now get $k(p) \mid \operatorname{ord}_{u'}(2)$, and thus there exists a $c \in \mathbb{N}$ such that $k(p) = \operatorname{ord}_{u'}(2)/c$. Suppose that $c \neq 1$. Then we have $F_{r-s} \equiv F_{r-s+\operatorname{ord}_{u'}(2)/c} \pmod{p}$, or equivalently,

$$2^{2^{r-s}} \equiv 2^{2^{r-s+\operatorname{ord}_{u'}(2)/c}} \pmod{p}. \tag{27}$$

Again, using (20), we find that (27) is equivalent to $g^{2^r t} \equiv g^{2^{r+\operatorname{ord}_{u'}(2)/c}t} \pmod{p}$ and, by part (ii) of Lemma 8, we get

$$2^r t \equiv 2^{r+\operatorname{ord}_{u'}(2)/c} t \pmod{p-1}. \tag{28}$$

As $p - 1 = 2^r t u'$, (28) implies $2^{\operatorname{ord}_{u'}(2)/c} \equiv 1 \pmod{u'}$. Hence, by part (i) of Lemma 8, we obtain $\operatorname{ord}_{u'}(2) \mid \operatorname{ord}_{u'}(2)/c$, which is a contradiction with $c \neq 1$. This proves (iii). $\square$

Example 16. Let $p = 41$. Then $p - 1 = 2^3 \cdot 5$. Hence, $r = 3$ and $u = 5$. Next, we have $\operatorname{ord}_{41}(2) = 20 = 2^2 \cdot 5$, and thus $(p-1)/\operatorname{ord}_p(2) = 2$. By Proposition 11 we now obtain $\operatorname{ind}_g(2) = 2$ for some primitive root g of 41 and, by direct calculation, we can find that $\operatorname{ind}_g(2) = 2$ if and only if $g \in \{17, 24\}$. Since $\operatorname{ind}_g(2) = 2$, we have $s = 1$, $t = 1$, and $u' = u/t = 5$. By part (ii) of Theorem 15, we now get $h(41) = r - s = 2$ and, from part (iii) of Theorem 15, we obtain $k(41) = \operatorname{ord}_5(2) = 4$. Finally, direct calculation verifies that

$$(F_n \bmod 41)_{n=0}^{\infty} = (3, 5, 17, 11, 19, 38, 17, 11, 19, 38, \ldots).$$

The following Lemma 17 is well-known.

Lemma 17. *Let $n \in \mathbb{N} \cup \{0\}$ and let p be an odd prime. Then the Fermat number F_n is divisible by p if and only if $\operatorname{ord}_p(2) = 2^{n+1}$.*

A proof of Lemma 17 can be found, for example, in [4, p. 37].

Let $F = \{3, 5, 17, 257, 641, 65537, 114689, \ldots\}$ be the set of all primes p such that p is a divisor of some Fermat number F_n, where $n \in \mathbb{N} \cup \{0\}$. Since every Fermat number F_n is divisible by at least one prime p and every two Fermat numbers are coprime by Goldbach theorem [4, p. 33], F is the infinite set.

Proposition 18. *Let p be a prime, $p \neq 2$. Then $p \in F$ if and only if $k(p) = 1$.*

Proof. Let $p - 1 = 2^r u$ where $r, u \in \mathbb{N}$ and let $2 \nmid u$.

First, assume that $p \in F$. Then, by Lemma 17, $\operatorname{ord}_p(2) = 2^q$ for some $q \in \mathbb{N}$ and, by part (i) of Lemma 8, we get $q \leq r$. Hence,

$$\frac{p-1}{\operatorname{ord}_p(2)} = 2^{r-q} u. \tag{29}$$

On the other hand, by Corollary 14, there exist uniquely determined $s \in \mathbb{N} \cup \{0\}$ and $t \in \mathbb{N}$ such that $0 \leq s \leq r$, $t \mid u$ and $2^s t = \operatorname{ind}_g(2)$ for some primitive root g of p. Applying (10), we now obtain

$$\frac{p-1}{\operatorname{ord}_p(2)} = \operatorname{ind}_g(2) = 2^s t.$$

This, along with (29), yields $2^{r-q} u = 2^s t$. Since $2 \nmid u$ and $2 \nmid t$, we have $u = t$. Hence, $u/t = 1$ and, by part (iii) of Theorem 15, we get $k(p) = 1$.

Conversely, let us assume that $k(p) = 1$. Then, by part (iii) of Theorem 15, we have $\operatorname{ord}_{u'}(2) = 1$, which implies $u' = 1$. As $u' = u/t$, we have $u = t$ and, by Corollary 14, $\operatorname{ind}_g(2) = 2^s u$ for some $s \in \mathbb{N} \cup \{0\}$ where $0 \leq s \leq r$. Next, applying (10), we obtain

$$\operatorname{ord}_p(2) = \frac{p-1}{\operatorname{ind}_g(2)} = \frac{2^r u}{2^s u} = 2^{r-s}. \tag{30}$$

Suppose now that $r - s = 0$. Then, by (30), $\operatorname{ord}_p(2) = 1$ which yields $2 \equiv 1 \pmod{p}$, a contradiction. Hence, $r - s \in \mathbb{N}$ and, $r - s - 1 \in \mathbb{N} \cup \{0\}$. Applying Lemma 17 to (30) we now get $p \mid F_{r-s-1}$, which means that $p \in F$. $\square$

Example 19. Let $p = 641$. Then $p - 1 = 2^7 \cdot 5$. Hence, $r = 7$ and, $u = 5$. Since $\operatorname{ord}_{641}(2) = 2^6$, by Lemma 17 we have $641 \mid F_5$. As $(p-1)/\operatorname{ord}_p(2) = 10$, by (10), we obtain $\operatorname{ind}_g(2) = 10$ for some primitive root g of 641 and direct calculation verifies that $\operatorname{ind}_g(2) = 10$ if and only if $g \in \{96, 108, 299, 304, 337, 342, 533, 545\}$. Hence, $s = 1$, $t = 5$ and $u' = u/t = 1$. Applying part (ii) and (iii) of Theorem 15, we now get $h(641) = r - s = 6$ and $k(641) = \operatorname{ord}_1(2) = 1$. Finally, we can verify that

$$(F_n \bmod 641)_{n=0}^{\infty} = (3, 5, 17, 257, 155, 0, 2, 2, 2, 2, 2, \ldots).$$

4 A simpler formulation of Aigner's theorem

In this section we find a simpler formulation of Aigner's result presented as Theorem 1. We show that the numbers $h(p)$ and $k(p)$ can be determined without resorting to the theory of primitive roots and indices. Our considerations are based only on the concept of a multiplicative order and its properties.

Theorem 20. *Let p be a prime, $p \neq 2$ and let* $\mathrm{ord}_p(2) = 2^v w$ *where* $v \in \mathbb{N} \cup \{0\}$, $w \in \mathbb{N}$ *and,* $2 \nmid w$. *Then we have*

(i) $h(p) = v$.

(ii) $k(p) = \mathrm{ord}_w(2)$.

Proof. We prove (i). First we show that

$$F_v \equiv F_{v+\mathrm{ord}_w(2)} \pmod{p}. \tag{31}$$

Since $\mathrm{ord}_p(2) = 2^v w$, from part (i) of Definition 7, we get

$$2^{\mathrm{ord}_w(2)} \equiv 1 \left(\mathrm{mod}\ \frac{\mathrm{ord}_p(2)}{2^v}\right). \tag{32}$$

By multiplying (32) by 2^v, we receive $2^{v+\mathrm{ord}_w(2)} \equiv 2^v \pmod{\mathrm{ord}_p(2)}$, which is, by part (ii) of Lemma 8, equivalent to $2^{2^{v+\mathrm{ord}_w(2)}} \equiv 2^{2^v} \pmod{p}$. Hence, (31) follows.

Next, applying Lemma 6 to (31), we obtain $v \equiv v + \mathrm{ord}_w(2) \pmod{k(p)}$, which yields $h(p) \leq v$ and $k(p) \mid \mathrm{ord}_w(2)$. Specifically, by taking $v = 0$ in $h(p) \leq v$, we get $h(p) = 0$. Let $v \neq 0$ and let $t \in \{0, \ldots, v-1\}$. Suppose now that $F_t \equiv F_v \pmod{p}$. Then $2^{2^t} \equiv 2^{2^v} \pmod{p}$ and, using part (ii) of Lemma 8, we obtain $2^t \equiv 2^v \pmod{\mathrm{ord}_p(2)}$. Since $\mathrm{ord}_p(2) = 2^v w$ we have $2^v w \mid 2^t(2^{v-t} - 1)$, which is a contradiction with $v > t$. Hence, $F_t \not\equiv F_v \pmod{p}$ for every $t \in \{0, \ldots, v-1\}$. This means that $h(p) \geq \#\{0, \ldots, v-1\} = v$, which along with $h(p) \leq v$, proves (i).

We prove (ii). By (31), $\mathrm{ord}_w(2)$ is the length of the period of $(F_n \bmod p)_{n=0}^{\infty}$ and, by Lemma 6, we have $k(p) \mid \mathrm{ord}_w(2)$. Therefore, there exists an $s \in \mathbb{N}$ such that $k(p) = \mathrm{ord}_w(2)/s$. Suppose that $s \neq 1$. From $F_v \equiv F_{v+k(p)} \pmod{p}$ now it follows that $2^{2^v} \equiv 2^{2^{v+\mathrm{ord}_w(2)/s}} \pmod{p}$ and, by part (ii) of Lemma 8, we obtain

$$2^v \equiv 2^{v+\mathrm{ord}_w(2)/s} \pmod{\mathrm{ord}_p(2)}.$$

This, together with $\mathrm{ord}_p(2) = 2^v w$, yields $2^{\mathrm{ord}_w(2)/s} \equiv 1 \pmod{w}$. Applying part (i) of Lemma 8, we now get $\mathrm{ord}_w(2) \mid \mathrm{ord}_w(2)/s$, which is a contradiction. Hence, we have $s = 1$ and the desired result follows. □

5 Some new results concerning the numbers $h(p)$

In this section, we take a closer look at the properties of the numbers $h(p)$ and show that part (i) of Theorem 20 can be refined substantially. We start by recalling some known properties of the quadratic character of 2.

Theorem 21. *Let p be a prime, $p \neq 2$. Then we have*

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod p \tag{33}$$

and,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv 1,7 \pmod 8; \\ -1, & \text{if } p \equiv 3,5 \pmod 8). \end{cases} \tag{34}$$

A proof of (33) can be found, for example, in the books [2, p. 176] or [6, p. 418] and, for a proof of (34), see [2, p. 180] or [6, p. 422].

Theorem 22. *For every prime p,* (i)–(iii) *hold.*

(i) *If $p \equiv 7 \pmod 8$, then $2 \nmid \mathrm{ord}_p(2)$. Consequently, $h(p) = 0$.*

(ii) *If $p \equiv 3 \pmod 8$, then $2 \parallel \mathrm{ord}_p(2)$. Consequently, $h(p) = 1$.*

(iii) *If $p \equiv 5 \pmod 8$, then $4 \parallel \mathrm{ord}_p(2)$. Consequently, $h(p) = 2$.*

Proof. We prove (i). If $p \equiv 7 \pmod 8$, then $p = 8\alpha + 7$ for an $\alpha \in \mathbb{N} \cup \{0\}$. Hence, $2^{(p-1)/2} = 2^{4\alpha+3}$. On the other hand, by Theorem 21, $2^{(p-1)/2} \equiv 1 \pmod p$. This means that $2^{4\alpha+3} \equiv 1 \pmod p$. By part (i) of Lemma 8, we now obtain $\mathrm{ord}_p(2) \mid 4\alpha + 3$. Hence, $2 \nmid \mathrm{ord}_p(2)$. Finally, applying part (i) of Theorem 20, we get $h(p) = 0$.

We prove (ii). If $p \equiv 3 \pmod 8$, then $p = 8\alpha + 3$ for an $\alpha \in \mathbb{N} \cup \{0\}$. Hence, $2^{(p-1)/2} = 2^{4\alpha+1}$. On the other hand, by Theorem 21, $2^{(p-1)/2} \equiv -1 \pmod p$. This means that $2^{4\alpha+1} \equiv -1 \pmod p$. Let $\mathrm{ord}_p(2) = u$. Suppose now that $2 \nmid u$. Then, by part (i) of Lemma 8, $u \mid p - 1 = 2(4\alpha + 1)$. This means that $u \mid 4\alpha + 1$. Therefore, there exists a $t \in \mathbb{N}$ such that $4\alpha+1 = tu$. Hence, $2^{4\alpha+1} = (2^u)^t \equiv 1^t \equiv 1 \pmod p$, which is a contradiction. Thus, we have $2 \mid u$, which, along with $u \mid 2(4\alpha+1)$, yields $2 \parallel \mathrm{ord}_p(2)$. Applying part (i) of Theorem 20, we now obtain $h(p) = 1$.

We prove (iii). If $p \equiv 5 \pmod 8$, then $p = 8\alpha + 5$ for an $\alpha \in \mathbb{N} \cup \{0\}$. Hence, $2^{(p-1)/2} = 2^{4\alpha+2}$. On the other hand, by Theorem 21, we have $2^{(p-1)/2} \equiv -1 \pmod p$. This means that $2^{4\alpha+2} \equiv -1 \pmod p$. Let $\mathrm{ord}_p(2) = u$. Suppose now that $4 \nmid u$. Then, by part (i) of Lemma 8, $u \mid p - 1 = 4(2\alpha + 1)$ and $u \mid 2\alpha + 1$ follows. Therefore, there exists a $t \in \mathbb{N}$ such that $2\alpha + 1 = tu$. Hence, $2^{4\alpha+2} = (2^u)^{2t} \equiv 1^{2t} \equiv 1 \pmod p$, which is a contradiction. Thus, $4 \mid u$, which, along with $u \mid 4(2\alpha+1)$, yields $4 \parallel \mathrm{ord}_p(2)$. Applying part (i) of Theorem 20, we now obtain $h(p) = 2$. □

The case of primes $p \equiv 1 \pmod 8$ solves Theorem 23.

Theorem 23. *For every $v \in \mathbb{N} \cup \{0\}$, there exists at least one prime $p \equiv 1 \pmod 8$ such that $h(p) = v$.*

Proof. Let us divide the proof into two parts. First, we show that the conclusion of Theorem 23 is true for every $v \in \{0, 1, 2\}$. Direct calculation verifies that (i)–(iii) hold.

(i) If $p = 73$, then $p \equiv 1 \pmod 8$ and $h(73) = 0$.

(ii) If $p = 281$, then $p \equiv 1 \pmod 8$ and $h(281) = 1$.

(iii) If $p = 41$, then $p \equiv 1 \pmod 8$ and $h(41) = 2$.

The values of the primes $p \equiv 1 \pmod 8$ shown in (i)–(iii) are the least values for which the equality $h(p) = v$ occurs. Secondly, we prove that Theorem 23 also applies for every $v \in \mathbb{N} \cup \{0\}$, $v \geq 3$. Let p be a prime such that $p \mid F_{v-1}$ where $v \geq 3$. Then, by Lemma 17, $\mathrm{ord}_p(2) = 2^v$. This, along with part (i) of Theorem 20, yields $h(p) = v$. Now it is clear from Theorem 22 that $p = 2$ or $p \equiv 1 \pmod 8$. Since $h(2) = 0$, we have $p \equiv 1 \pmod 8$, as required. □

We conclude our study of Fermat numbers by presenting the tables of $h(p)$ and $k(p)$ for all primes $p < 1000$. The tables are shown in the Appendix.

6 Acknowledgment

The author thanks the anonymous referee for carefully reading the manuscript.

A Appendix: Tables of the values of $h(p)$ and $k(p)$ for $p < 1000$

p	$h(p)$	$k(p)$	p	$h(p)$	$k(p)$	p	$h(p)$	$k(p)$
2	0	1	3	1	1	5	2	1
7	0	2	11	1	4	13	2	2
17	3	1	19	1	6	23	0	10
29	2	3	31	0	4	37	2	6
41	2	4	43	1	3	47	0	11
53	2	12	59	1	28	61	2	4
67	1	10	71	0	12	73	0	6
79	0	12	83	1	20	89	0	10
97	4	2	101	2	20	103	0	8
107	1	52	109	2	6	113	2	3
127	0	3	131	1	12	137	2	8
139	1	22	149	2	36	151	0	4
157	2	12	163	1	54	167	0	82

p	$h(p)$	$k(p)$	p	$h(p)$	$k(p)$	p	$h(p)$	$k(p)$
173	2	14	179	1	11	181	2	12
191	0	36	193	5	2	197	2	21
199	0	30	211	1	12	223	0	36
227	1	28	229	2	18	233	0	28
239	0	24	241	3	2	251	1	20
257	4	1	263	0	130	269	2	66
271	0	36	277	2	11	281	1	12
283	1	23	293	2	9	307	1	8
311	0	20	313	2	12	317	2	39
331	1	4	337	0	6	347	1	172
349	2	28	353	3	10	359	0	178
367	0	60	373	2	10	379	1	18
383	0	95	389	2	48	397	2	10
401	3	20	409	2	8	419	1	90
421	2	12	431	0	14	433	3	6
439	0	9	443	1	24	449	5	3
457	2	18	461	2	44	463	0	30
467	1	29	479	0	119	487	0	162
491	1	84	499	1	82	503	0	50
509	2	7	521	2	12	523	1	84
541	2	36	547	1	12	557	2	138
563	1	70	569	2	35	571	1	18
577	4	6	587	1	292	593	2	36
599	0	132	601	0	20	607	0	100
613	2	24	617	1	30	619	1	102
631	0	12	641	6	1	643	1	106
647	0	72	653	2	162	659	1	69
661	2	20	673	4	2	677	2	156
683	1	10	691	1	44	701	2	60
709	2	58	719	0	179	727	0	110
733	2	60	739	1	20	743	0	156
751	0	100	757	2	18	761	2	36
769	7	2	773	2	96	787	1	130
797	2	99	809	2	100	811	1	36
821	2	20	823	0	68	827	1	174
829	2	66	839	0	418	853	2	70
857	2	106	859	1	60	863	0	43
877	2	18	881	0	20	883	1	42
887	0	442	907	1	30	911	0	12
919	0	24	929	4	28	937	0	12
941	2	92	947	1	70	953	2	8
967	0	66	971	1	48	977	3	60
983	0	490	991	0	60	997	2	82

References

[1] A. Aigner, Über Primzahlen, nach denen (fast) alle Fermatschen Zahlen quadratische Nichtreste sind, *Monatsh. Math.* **101** (1986), 85–93.

[2] D. M. Burton, *Elementary Number Theory*, 7th edition, McGraw-Hill, 2011.

[3] E. Deza, *Mersenne Numbers and Fermat Numbers, Selected Chapters of Number Theory: Special Numbers*, World Scientific, 2021.

[4] M. Křížek, F. Luca, and L. Somer, 17 *Lectures on Fermat Numbers, From Number Theory to Geometry*, Canadian Mathematical Society, Springer, 2001.

[5] B. Rittaud and A. Heeffer, The pigeonhole principle, two centuries before Dirichlet, *Math. Intell.* **36** (2014), 27–29.

[6] K. H. Rosen, *Elementary Number Theory and Its Applications*, Sixth Edition, Addison-Wesley, 2011.

[7] N. J. A. Sloane et al., The On-Line Encyclopedia of Integer Sequences, available at `https://oeis.org`, 2024.

[8] I. M. Vinogradov, *Elements of Number Theory*, Dover Publications, 1954.

2020 *Mathematics Subject Classification:* Primary 11B50; Secondary 11B83, 11A41.
Keywords: Fermat number, modular periodicity, pre-period, primitive period.

(Concerned with sequences A000215 and A102742.)

Received June 18 2024; revised version received April 29 2025. Published in *Journal of Integer Sequences*, December 15 2025.

Return to Journal of Integer Sequences home page.