Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. 50(4)(2018) pp. 1-21

Gauss Factorials, Jacobi Primes, and Generalized Fermat Numbers

John B. Cosgrave
79 Rowanbyrn,
Blackrock, County Dublin, A94 FF86, Ireland.
Email: jbcosgrave@gmail.com

Karl Dilcher
Department of Mathematics and Statistics,
Dalhousie University,
Halifax, Nova Scotia, B3H 4R2, Canada.
Email: dilcher@mathstat.dal.ca

Received: 24 May, 2017 / Accepted: 14 July, 2017 / Published online: 25 April, 2018

Abstract. Given positive integers N and n, we define the Gauss factorial $N_n!$ as the product of all positive integers from 1 to N and coprime to n. In this expository paper we begin with the classical theorem of Wilson, extending it in various different but related directions, mostly modulo composite integers. Most of the results presented in this paper involve the multiplicative orders, and in particular order 1, of certain Gauss factorials. In the process we define two types of special primes, the Gauss and Jacobi primes, and some of the results involve large-scale computations, including factoring certain generalized Fermat numbers. The main tools in most of the results are the well-known binomial coefficient theorems of Gauss and Jacobi, along with other related congruences and their generalizations.

AMS (MOS) Subject Classification Codes: 11A07; 11B65
Key Words: Gauss-Wilson theorem, Gauss factorials, binomial coefficient congruences, generalized Fermat numbers, factors.

1. Introduction

1.1. In this expository paper we present a variety of results around the common theme of *Gauss factorials*, objects from elementary number theory that have long been known, though not under this name. In a sequence of papers published over the last 10 years, we showed that Gauss factorials, in spite of their very simple definition, have a remarkably rich structure. On the one hand, they proved to be particularly useful in extending some known deep theorems, while on the other hand they have led us to new and often unexpected results.

We begin with *Wilson's theorem*, which, along with its converse by Lagrange, is one of the most important and best-known results in the elementary theory of numbers: p is a prime exactly when

$$(p-1)! \equiv -1 \pmod{p}. \tag{1. 1}$$

An easy proof of Wilson's theorem, which is given in most elementary number theory books, relies on the fact that if $a \in \mathbb{N}$ satisfies $1 < a < p-1$, then a^{-1} is not equivalent to a modulo p.

For an odd prime p we now write out $(p-1)!$ explicitly and use symmetry; we then obtain

$$1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2}\,\tfrac{p+1}{2} \cdot \ldots \cdot (p-1) \equiv \left(\tfrac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)! \pmod{p}, \tag{1. 2}$$

and thus, with (1. 1),

$$\left(\tfrac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}. \tag{1. 3}$$

According to [19, p. 275], this was first observed by Lagrange. If $p \equiv 1 \pmod 4$, then the right side of the congruence (1. 3) is -1; this implies

$$\operatorname{ord}_p\left(\left(\tfrac{p-1}{2}\right)!\right) = 4 \quad \text{for} \quad p \equiv 1 \pmod 4. \tag{1. 4}$$

(Here and elsewhere in this paper, $\operatorname{ord}_p(a)$ stands for the multiplicative order, modulo p, of the element a.) On the other hand, when $p \equiv 3 \pmod 4$ the congruence (1. 3) implies

$$\left(\tfrac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}. \tag{1. 5}$$

It is a rather non-trivial matter to determine the sign on the right. In fact, given a prime $p \equiv 3 \pmod 4$ and $p > 3$, Mordell [30] proved

$$\left(\tfrac{p-1}{2}\right)! \equiv -1 \pmod{p} \qquad \text{if and only if} \qquad h(-p) \equiv 1 \pmod 4, \tag{1. 6}$$

where $h(-p)$ denotes the class number of $\mathbb{Q}(\sqrt{-p})$. In his paper [30], Mordell notes that Chowla had independently discovered this result. A proof can also be found in [35, Theorem 8], as well as in a book by Venkov, both in the translated edition [36, p. 9] of 1970 and in the original, published in Russian in 1937. No reference is given, so Venkov may have been the first to prove the relationship (1. 6). With this result, the multiplicative order of $\left(\frac{p-1}{2}\right)!$ modulo p is now completely determined:

Corollary 1.1. *Let $p > 2$ be a prime. Then*

$$\operatorname{ord}_p\left(\left(\tfrac{p-1}{2}\right)!\right) = \begin{cases} 4 & \textit{if} \quad p \equiv 1 \pmod 4, \\ 2 & \textit{if} \quad p \equiv 3 \pmod 4,\ p > 3, \\ & \qquad \textit{and } h(-p) \equiv 1 \pmod 4, \\ 1 & \textit{otherwise}. \end{cases} \tag{1. 7}$$

1.2. The above results and observations lead to the natural question of whether there are analogues for *composite* moduli. Indeed, we have a generalization of Wilson's theorem, first obtained by Gauss. Before stating it, we introduce some key notation:

Let N and n be positive integers. We write $N_n!$ for the product of all positive integers up to N that are coprime to n, i.e.,

$$N_n! = \prod_{\substack{1\le j\le N\\ \gcd(j,n)=1}} j. \tag{1. 8}$$

A similar notation was introduced in [22], a useful reference on congruences for factorials and binomial coefficients. We call $N_n!$ a *Gauss factorial*. This terminology is related to the following theorem of Gauss.

Theorem 1.2 (Gauss)**.** *Given an integer $n \ge 2$, we have*

$$(n-1)_n! \equiv \begin{cases} -1 \pmod n & \text{for} \quad n = 2, 4, p^\alpha, \text{ or } 2p^\alpha, \\ 1 \pmod n & \text{otherwise}, \end{cases} \tag{1. 9}$$

where $p > 2$ is a prime and $\alpha \ge 1$ an integer.

This congruence is also known as the Gauss-Wilson Theorem. The first case of (1. 9) occurs if and only if n has a primitive root. Numerous references can be found in [19, p. 65]. Although this result was first stated in the celebrated *Disquisitiones Arithmeticae* [21, §78] and occurs in the well-known books [20, §38] and [23, p. 102], in general it is surprising how little information on this topic can be found in the literature. The few published papers on Theorem 1.2 include [25] and [33], where Theorem 1 was further extended. Also, the congruence (1. 9) was used in [26] and in [1] to extend the well-known *Wilson quotient* (see (3. 3) below) to composite moduli. At least once Theorem 1.2 was rediscovered; see [32].

The Gauss-Wilson Theorem and the concept of Gauss factorial now make it possible to extend (1. 7) to arbitrary composite (but odd) moduli.

Theorem 1.3. *Given an odd integer $n \ge 3$, we assume that $p \ne q$ are odd primes and α, β are positive integers. Then*
(1) $\operatorname{ord}_n\big((\frac{n-1}{2})_n!\big) = 4$ *when* $n = p^\alpha$ *and* $p \equiv 1 \pmod 4$*;*
(2) $\operatorname{ord}_n\big((\frac{n-1}{2})_n!\big) = 2$ *when*

- (a) $n = p^{2\alpha-1}$, $p \equiv 3 \pmod 4$, $p > 3$, *and* $h(-p) \equiv 1 \pmod 4$, *or*
- (b) $n = p^{2\alpha}$, $p = 3$, *or* $p \equiv 3 \pmod 4$ *and* $h(-p) \not\equiv 1 \pmod 4$, *or*
- (c) $n = p^\alpha q^\beta$ *and* p *or* $q \equiv 3 \pmod 4$,
- (d) $n = p^\alpha q^\beta$, $p \equiv q \equiv 1 \pmod 4$, *and* p *is a quadratic nonresidue* $\pmod q$*;*

(3) $\operatorname{ord}_n\big((\frac{n-1}{2})_n!\big) = 1$ *in all other cases.*

This result was proved in [8], with some extensions and generalizations. We note in passing that by the quadratic reciprocity law, the condition "p is a quadratic nonresidue $\pmod q$" in part 2(d) means that q is also a quadratic nonresidue $\pmod p$.

Example 1. Let $n = 3 \cdot 5 \cdot 7 = 105$; then we compute

$$(\frac{n-1}{2})_n! = 1 \cdot 2 \cdot 4 \cdot 8 \cdot 11 \cdot 13 \cdot 17 \cdots 44 \cdot 46 \cdot 47 \cdot 52 \equiv 1 \pmod{105},$$

which is consistent with part (3) of Theorem 3.1.

1.3. The questions and results mentioned above are the first instances of our general long-term program that has the aim of studying, as completely as possible, the special Gauss factorials

$$\left(\frac{n-1}{M}\right)_n !, \quad M \geq 1, \quad n \equiv 1 \pmod{M}, \tag{1. 10}$$

where M is a positive integer. In particular we are interested in their multiplicative orders (mod n), but also, if possible, in their values (mod n).

We now provide a brief summary, which can also be seen as a preview of some of what follows in the remainder of this paper:

$M = 1$: This is just Theorem 1.2 (Gauss-Wilson).

$M = 2$: This is Theorem 1.3; the only possible orders are 1, 2, and 4.

$M \geq 3$: The orders are generally unbounded. Various partial results are known; for instance,

- If n has *three or more* different prime factors $\equiv 1 \pmod{M}$, then $(\frac{n-1}{M})_n! \equiv 1 \pmod{n}$.
- If n has *two* different prime factors $\equiv 1 \pmod{M}$, then the order of $(\frac{n-1}{M})_n!$ divides M.
- If n has *one* prime factor $\equiv 1 \pmod{M}$: This is the most interesting case; we will present three different instances of this in the present paper.
- If n has *no* prime factor $\equiv 1 \pmod{M}$: This case seems utterly intractable.

We conclude this introduction with two remarks related to the outline above:

1. Other partial products of the "full" product $(n-1)_n!$ have also been studied by the present authors [11].

2. There are some meaningful results also when $n \not\equiv 1 \pmod{M}$; in this case we consider $\lfloor \frac{n-1}{M} \rfloor_n !$.

2. Binomial Coefficient Congruences

2.1. In this section we give a first application of Gauss factorials. Most of what follows can be found in [9], with proofs.

One of the most remarkable results on binomial coefficients is a congruence due to Gauss (1828). It relies on the celebrated theorem of Fermat which states that p can be represented as a sum of two squares exactly when $p \equiv 1 \pmod{4}$, uniquely up to signs and the order of the summands. Let us now fix p and a such that

$$p = a^2 + b^2, \qquad p \equiv 1 \pmod{4}, \qquad a \equiv 1 \pmod{4}. \tag{2. 1}$$

We can now state Gauss's theorem:

Theorem 2.1 (Gauss)**.** *Let the prime p and the integer a be as in* (2. 1)*. Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod{p}. \tag{2. 2}$$

For a proof and generalizations of this result see, e.g., [5, p. 268]. Beukers [4] first conjectured an extension to a congruence modulo p^2, and this was first proved in [6].

Theorem 2.2 (Chowla, Dwork, Evans)**.** *Let p, a be as in* (2. 1)*. Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \left(1 + \tfrac{1}{2}pq_p(2)\right)\left(2a - \tfrac{p}{2a}\right) \pmod{p^2}. \tag{2. 3}$$

Here $q_p(m)$ is the *Fermat quotient* with base m ($p \nmid m$), defined for primes $p > 2$ by

$$q_p(m) := \frac{m^{p-1} - 1}{p}. \tag{2. 4}$$

Congruences such as (2. 3) have been very useful in large-scale computations to search for Wilson primes; see [17] or [18].

Only a few years after Gauss proved his celebrated result, Jacobi proved the following analogous theorem. We fix a prime $p > 2$ and integers r, s so that

$$4p = r^2 + 3s^2, \quad p \equiv 1 \pmod 6, \quad r \equiv 1 \pmod 3, \quad s \equiv 0 \pmod 3. \tag{2. 5}$$

The integer r is then uniquely determined. The following congruence, analogous to Gauss's Theorem 2.1, is due to Jacobi (1837); see [5, p. 291] for remarks and references.

Theorem 2.3 (Jacobi)**.** *With p, r as in* (2. 5)*, we have*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p. \tag{2. 6}$$

In analogy to Theorems 2.1 and 2.2, this congruence has also been extended, by Evans and independently by Yeung; see [5, p. 293] for remarks and references.

Theorem 2.4 (Evans; Yeung)**.** *With p, r as in* (2. 5)*, we have*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r + \frac{p}{r} \pmod{p^2}. \tag{2. 7}$$

For the usefulness of this congruence, see again [17] or [18].

2.2. The point of the paper [9] was to show that Gauss factorials can be used to extend the theorems of Gauss and Jacobi in a somewhat different direction from Theorems 2.2 and 2.4. But subsequently, as consequences we recover these two extensions, along with modulo p^3 extensions.

More specifically, the following two results are obtained in [9].

Theorem 2.5. *Let p and a be as in* (2. 1) *and let $\alpha \geq 2$ be an integer. Then*

$$\frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2} \equiv 2a - C_0\frac{p}{2a} - C_1\frac{p^2}{8a^3} - \ldots - C_{\alpha-2}\frac{p^{\alpha-1}}{(2a)^{2\alpha-3}} \pmod{p^\alpha}, \tag{2. 8}$$

where $C_n := \frac{1}{n+1}\binom{2n}{n}$ is the nth Catalan number.

The first few Catalan numbers are 1, 1, 2, 5, 14, and 42; they are all integers.

Theorem 2.6. *Let p and r be as in* (2. 5) *and let $\alpha \geq 2$ be an integer. Then*

$$\frac{\left(\frac{2(p^\alpha-1)}{3}\right)_p!}{\left(\left(\frac{p^\alpha-1}{3}\right)_p!\right)^2} \equiv -r + C_0\frac{p}{r} + C_1\frac{p^2}{r^3} + \ldots + C_{\alpha-2}\frac{p^{\alpha-1}}{r^{2\alpha-3}} \pmod{p^\alpha}. \tag{2. 9}$$

The proofs of these theorems are similar to each other, and involve some deep theorems connecting the p-adic gamma function of Morita with Jacobi sums.

The left sides of (2. 8) and (2. 9) can be seen as analogous to binomial coefficients, and in fact, for $\alpha = 1$, both theorems reduce to the theorems of Gauss and Jacobi, respectively. Furthermore, using evaluations modulo p of certain finite sums of reciprocals, for $\alpha = 2$ the two theorems above easily lead to Theorem 2.2 and 2.4, respectively. Finally, using further congruences for sums of reciprocals, this time mainly modulo p^2, we obtain the following two results:

Theorem 2.7. *With p, a as in* (2. 1)*, we have*

$$\begin{aligned}\binom{\frac{p-1}{2}}{\frac{p-1}{4}} &\equiv \left(2a - \frac{p}{2a} - \frac{p^2}{8a^3}\right) \\ &\quad \times \left(1 + \tfrac{1}{2}pq_p(2) + \tfrac{1}{8}p^2\left(2E_{p-3} - q_p(2)^2\right)\right) \pmod{p^3}.\end{aligned} \tag{2. 10}$$

Here E_n denotes the nth Euler number which can be defined by

$$\frac{2}{e^t + e^{-t}} = \sum_{n=0}^{\infty} \frac{E_n}{n!}t^n \qquad (|t| < \pi).$$

The sequence of Euler numbers, for $n \geq 0$, begins with 1, 0, -1, 0, 5, 0, -61, and we have $E_{2j+1} = 0$ for $j \geq 0$; they are all integers.

Theorem 2.8. *Let p, r be as in* (2. 5)*. Then*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv \left(-r + \frac{p}{r} + \frac{p^2}{r^3}\right)\left(1 + \frac{1}{6}p^2B_{p-2}(\tfrac{1}{3})\right) \pmod{p^3}. \tag{2. 11}$$

Here $B_n(x)$ is the nth Bernoulli polynomial, defined by

$$\frac{te^{tx}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!} \qquad (|t| < 2\pi).$$

As examples of the summation congruences that are used for deriving (2. 3) and (2. 10) from (2. 8), respectively (2. 7) and (2. 11) from (2. 9), we mention only

$$\sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j} \equiv -2q_p(2) + pq_p(2)^2 \pmod{p^2}, \tag{2. 12}$$

and for $p \equiv 1 \pmod 4$,

$$\sum_{1 \leq j < k \leq \frac{p-1}{4}} \frac{1}{jk} \equiv \tfrac{9}{2}q_p(2)^2 - 2E_{p-3} \pmod{p}, \tag{2. 13}$$

both valid for primes $p \geq 5$; see Lemmas 2 and 3 in [9]. Congruences of this type have a long history that goes back to the 19th century, with important work by Glaisher and then E. Lehmer [28]. More recent work on this is due to Sun [34], and a systematic treatment can be found in [2]. Such congruences exist also for composite moduli; see, e.g., [12, 13] and the references contained in these papers.

To conclude this section, we mention that an analogue to Gauss's and to Jacobi's theorem is due to Hudson and Williams [24], and its "Catalan extension", i.e., a result analogous to Theorems 2.5 and 2.6, was obtained in [15]; see Theorems 3.4 and 3.5 below. Finally, a systematic study of numerous congruences of the type of Gauss, Jacobi, and Hudson and Williams can be found in [5]. By using the methods of [9], their corresponding "Catalan extensions" were recently obtained in [3].

3. Sequences of Multiplicative Orders

3.1. In our second application of Gauss factorials, we will consider certain sequences of multiplicative orders. Most of the material in this section, expanded and with proofs, can be found in [10] and [15].

Given $M \geq 2$ and a prime number $p \equiv 1 \pmod{M}$, our main objects of study will be the orders

$$\gamma_\alpha^{(M)}(p) := \operatorname{ord}_{p^\alpha} \left(\left(\tfrac{p^\alpha - 1}{M} \right)_{p^\alpha} ! \right). \tag{3. 1}$$

We typically fix M and p, and let α vary. Note that, clearly,

$$\left(\tfrac{p^\alpha - 1}{M} \right)_{p^\alpha} ! = \left(\tfrac{p^\alpha - 1}{M} \right)_{p} !, \qquad \alpha = 1, 2, 3, \ldots,$$

so from here on we will use the simpler form on the right.

We begin by considering $M = 4$ and $p = 5$, the smallest possible prime. For greater ease of notation we set, for now, $\gamma_\alpha := \gamma_\alpha^{(4)}(p)$. Then obviously we have $\gamma_1 = 1$, and computations using Maple [29] show that $\gamma_2 = 10$, $\gamma_3 = 25$, $\gamma_4 = 250$, $\gamma_5 = 625$, and $\gamma_6 = 6250$. To further explore this pattern, we display the first few values of γ_α in Table 1, for the first five prime numbers $p \equiv 1 \pmod{4}$. The lower part of the table (using, for simplicity, $\gamma = \gamma_1$) shows quite clearly how, given a prime p, the order $\gamma_{\alpha+1}$ appears to depend on the previous order γ_α.

α/p	5	13	17	29	37
1	1	12	16	7	18
2	10	156	272	406	333
3	25	2 028	4 624	5 887	24 642
4	250	26 364	78 608	341 446	455 877
5	625	342 732	1 336 336	4 950 967	33 734 898
1	γ	γ	γ	γ	γ
2	$2p\gamma$	$p\gamma$	$p\gamma$	$2p\gamma$	$\frac{1}{2}p\gamma$
3	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$
4	$2p^3\gamma$	$p^3\gamma$	$p^3\gamma$	$2p^3\gamma$	$\frac{1}{2}p^3\gamma$
5	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$

Table 1: $\gamma_\alpha = \gamma_\alpha^{(4)}(p)$ for $1 \leq \alpha \leq 5$ and $p \leq 37$, $p \equiv 1 \pmod{4}$.

Further computations might lead one to conjecture that, given a prime $p \equiv 1 \pmod 4$ and $\gamma := \operatorname{ord}_p(\frac{p-1}{4}!)$, the sequence of orders $\gamma_1 = \gamma, \gamma_2, \gamma_3, \dots$ is

$$\begin{cases} \gamma, p\gamma, p^2\gamma, p^3\gamma, \dots & \text{when } p \equiv 1 \pmod 8 \\ & \quad \text{or } p \equiv 5 \pmod 8 \text{ and } 4|\gamma, \\ \gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \dots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \equiv 2 \pmod 4, \\ \gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \dots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \text{ is odd.} \end{cases} \tag{3. 2}$$

However, for $p = 29\,789$ this pattern fails: We have $\gamma_1 = 14\,894$, while $\gamma_2 = 7\,447$. That is, in the step from γ_1 to γ_2, there was no factor p.

In addition to discussing the pattern (3. 2), this section will be concerned with "exceptional primes" such as $p = 29\,789$, and we will address the following natural questions:

– Are there more?

– Can we characterize and/or compute them?

– Can the "skipped p" occur elsewhere in the sequence?

3.2. Now we return to the general case $M \geq 2$ in (3. 1). The next result shows that the pattern (3. 2), which we observed for $M = 4$, is actually true in general.

Theorem 3.1. *Given integers $M \geq 2$ and $\alpha \geq 1$, and a prime $p \equiv 1 \pmod M$, let $\gamma_\alpha^{(M)}(p)$ be as in* (3. 1). *If $p \equiv 1 \pmod{2M}$, then*

$$\gamma_{\alpha+1}^{(M)}(p) = p\gamma_\alpha^{(M)}(p) \quad \textit{or} \quad \gamma_{\alpha+1}^{(M)}(p) = \gamma_\alpha^{(M)}(p).$$

If $p \equiv M + 1 \pmod{2M}$, then

$$\gamma_{\alpha+1}^{(M)}(p) = \begin{cases} p\gamma_\alpha^{(M)}(p) \quad \textit{or} \quad \gamma_\alpha^{(M)}(p) & \textit{when} \quad \gamma_\alpha^{(M)}(p) \equiv 0 \pmod 4, \\ \frac{1}{2}p\gamma_\alpha^{(M)}(p) \quad \textit{or} \quad \frac{1}{2}\gamma_\alpha^{(M)}(p) & \textit{when} \quad \gamma_\alpha^{(M)}(p) \equiv 2 \pmod 4, \\ 2p\gamma_\alpha^{(M)}(p) \quad \textit{or} \quad 2\gamma_\alpha^{(M)}(p) & \textit{when} \quad \gamma_\alpha^{(M)}(p) \equiv 1 \pmod 2. \end{cases}$$

This leads to the following definition.

Definition 3.2. *When the second alternative holds in one of the cases in Theorem 3.1, we call p an α-exceptional prime for M.*

It turns out that exceptional primes are extremely rare. Table 2 shows all that are known to us, with their respective search limits. For $49 \leq M \leq 100$ there are no 1-exceptional primes $p \leq 2 \cdot 10^6$; we'll consider the case $\alpha \geq 2$ a bit later.

In order to explain how the entries in Table 2 were computed, we establish two different criteria for exceptionality, the first of which — while completely general and effective — is computationally expensive in practice, and the second of which is very specialized (for the cases $M = 3, 4$ and 6), but is extremely fast in application.

M	p	up to
3	13, 181, 2 521, 76 543, 489 061	10^{12}
4	29 789	10^{11}
5	71	$2 \cdot 10^6$
6	13, 181, 2 521, 76 543, 489 061	10^{12}
10	11	$2 \cdot 10^6$
18	1 090 891	$2 \cdot 10^6$
21	211, 15 583	$2 \cdot 10^6$
23	3 037	$2 \cdot 10^6$
24	73	$2 \cdot 10^6$
29	59	$2 \cdot 10^6$
35	1 471	$2 \cdot 10^6$
44	617	$2 \cdot 10^6$
48	97	$2 \cdot 10^6$

Table 2: 1-exceptional primes p for $3 \le M \le 100$.

For the first criterion, we need the following definitions. For any prime p, the *Wilson quotient* is defined by

$$w(p) := \frac{(p-1)! + 1}{p}. \tag{3. 3}$$

This is always an integer, by Wilson's Theorem (1. 1). This quotient, along with the Fermat quotient (2. 4), were of some importance in the study of Fermat's last theorem (in its classical theory; see, e.g., [31]). Next, for $M \ge 2$ and $p \equiv 1 \pmod{M}$, we define

$$S^M(p) := \sum_{j=1}^{\frac{p-1}{M}} \frac{1}{j}.$$

For $M = 2$, 3, 4 and 6 there are well-known evaluations in terms of Fermat quotients, e.g.,

$$\sum_{j=1}^{\frac{p-1}{4}} \frac{1}{j} \equiv -3q_p(2) \pmod{p}, \qquad \sum_{j=1}^{\frac{p-1}{3}} \frac{1}{j} \equiv -\tfrac{3}{2}q_p(3) \pmod{p}.$$

These identities are of the same nature as (2. 12) and (2. 13) and can be found, e.g., in [28] or [2].

Next, for $\alpha \ge 1$, $M \ge 2$ and $p \equiv 1 \pmod{M}$ we define $V_\alpha^M(p)$ by

$$\left(\left(\tfrac{p^\alpha - 1}{M} \right)_p ! \right)^{\gamma_\alpha^{(M)}(p)} \equiv 1 + V_\alpha^M(p) p^\alpha \pmod{p^{\alpha+1}}.$$

With these definitions and notations, we can state our first criterion for a prime to be α-exceptional for M.

Theorem 3.3. *The first alternative in each case of Theorem 3.1 holds exactly when*

$$V_\alpha^M(p) + \tfrac{1}{M}\gamma_\alpha^{(M)}(p)\left(w(p) - S^M(p)\right) \not\equiv 0 \pmod{p}.$$

The basic idea for the proofs of both Theorems 3.1 and 3.3 is as follows: First we establish a congruence connecting

$$\left(\tfrac{p^{\alpha+1}-1}{M}\right)_p ! \qquad \text{and} \qquad \left(\tfrac{p^{\alpha}-1}{M}\right)_p ! \pmod{p^{\alpha+1}}.$$

Then we raise both sides to an appropriate power, and finally use the definition of order. For details, see [10].

All entries in Table 2 were found by way of this criterion. However, its implementation proved too slow to reach the search limits listed for $M = 3, 4$ and 6, which were attained using the second, more specialized criterion; this will be explained later.

3.3. In the cases $M = 3, 4$ and 6 we can use the theory of Jacobi sums to obtain some strong criteria, in addition to further insight. For instance, the fact that the entries for $M = 3$ and 6 in Table 2 are identical will be explained in the process. For reasons of brevity, we will concentrate on $M = 3, 6$; the case $M = 4$ is similar, and details can be found in [15].

Suppose now that $p \equiv 1 \pmod 6$ is a prime. It is known that the representation $p = a^2 + 3b^2$ is unique up to sign, but the signs are crucial here. We fix them as follows: Let g be a primitive root modulo p, and choose a character χ_6 modulo p of order 6 in such a way that $\chi_6(g) = e^{2\pi i/6} = (1 + i\sqrt{3})/2$. Then we fix the signs of a and b by requiring that

$$a \equiv -1 \pmod 3, \qquad 3b \equiv (2g^{(p-1)/3} + 1)a \pmod p.$$

If a, b are given as above, we define two pairs r, s and u, v (in this exposition we need only r and u):

Let $Z = \text{ind}_g 2$, the index of $2 \pmod p$ with respect to the primitive root g. Then we have

$$\begin{cases} r = 2a, & u = 2a & (Z \equiv 0 \pmod 3), \\ r = -a - 3b, & u = -a + 3b & (Z \equiv 1 \pmod 3), \\ r = -a + 3b, & u = -a - 3b & (Z \equiv 2 \pmod 3). \end{cases} \tag{3. 4}$$

They also satisfy sums-of-squares identities:

$$4p = r^2 + 3s^2, \qquad 4p = u^2 + 3v^2, \qquad r \equiv u \equiv 1 \pmod 3.$$

We already encountered the number r in (2. 5) and in Theorem 2.3 and its generalizations. The number u, on the other hand, occurs in the following analogue of the theorems of Gauss and Jacobi [24]:

Theorem 3.4 (Hudson, Williams, 1984)**.** *With $p \equiv 1 \pmod 6$ prime and u as given in* (3. 4)*, we have*

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1} u \pmod p.$$

As already indicated in Section 2, this result also has a “Catalan extension”; as before, let $C_n := \frac{1}{n+1}\binom{2n}{n}$ be the nth Catalan number.

Theorem 3.5. *Let p and u be as in* (3. 4)*. Then for any integer $\alpha \geq 1$ we have*

$$\frac{\left(\frac{p^\alpha-1}{3}\right)_p!}{\left(\left(\frac{p^\alpha-1}{6}\right)_p!\right)^2} \equiv (-1)^{\frac{p-1}{6}+1}\left(u - \frac{p}{u} - \frac{p^2}{u^3} - \cdots - C_{\alpha-1}\frac{p^{\alpha-1}}{u^{2\alpha-3}}\right) \pmod{p^\alpha}.$$

The next result will be the basis for everything in the remainder of this section.

Theorem 3.6. *Let $p \equiv 1 \pmod 6$ and r, u as in* (3. 4)*. Then for all $\alpha \geq 1$ we have*

$$\left(r - \frac{p}{r} - \cdots - \frac{C_{\alpha-1}p^\alpha}{r^{2\alpha-1}}\right)^3 \equiv \left(u - \frac{p}{u} - \cdots - \frac{C_{\alpha-1}p^\alpha}{u^{2\alpha-1}}\right)^3 \pmod{p^{\alpha+1}}, \quad (3.\ 5)$$

where C_n is again the nth Catalan number.

The main ingredients in the proof are an identity between the cubes of certain Jacobi sums, as well as congruences (mod $p^{\alpha+1}$) between these Jacobi sums and both sides of the congruence (3. 5). Quotients of certain Gauss factorials are also involved as intermediate steps. For details, see Section 3 in [15].

By cubing the congruences in Theorems 2.6 and 3.5, and applying Theorem 3.6, we get the following result after some easy manipulations:

Corollary 3.7. *For any $p \equiv 1 \pmod 6$ and $\alpha \geq 1$ we have*

$$\left(\left(\frac{p^\alpha-1}{3}\right)_p!\right)^{24} \equiv \left(\left(\frac{p^\alpha-1}{6}\right)_p!\right)^{12} \pmod{p^\alpha}.$$

After some further intermediate steps, this in turn implies a result that explains why the entries for $M = 3$ and $M = 6$ in Table 2 are identical:

Corollary 3.8. *Let $p \equiv 1 \pmod 6$ and $\alpha \geq 1$. Then p is α-exceptional for $M = 3$ exactly when it is α-exceptional for $M = 6$.*

Another consequence of Theorem 3.6 is the second exceptionality criterion, for the special cases $M = 3$ and 6:

Theorem 3.9. *Let $p \equiv 1 \pmod 6$ and u be as in* (3. 4)*. Then for a fixed $\alpha \geq 1$, p is α-exceptional for $M = 3$ (and $M = 6$) exactly when*

$$\left(u - \frac{p}{u} - \frac{p^2}{u^3} - 2\frac{p^3}{u^5} - \cdots - C_{\alpha-1}\frac{p^\alpha}{u^{2\alpha-1}}\right)^{p-1} \equiv 1 \pmod{p^{\alpha+1}},$$

where C_n is the nth Catalan number.

The following important special case is worth mentioning:

Corollary 3.10. *Let $p \equiv 1 \pmod 6$ and u be as in* (3. 4)*. Then p is 1-exceptional for $M = 3$ (and $M = 6$) exactly when*

$$\left(u - \tfrac{p}{u}\right)^{p-1} \equiv 1 \pmod{p^2}.$$

In the case of 1-exceptionality, u can be replaced by $2a$ in the above result, and we obtain a particularly convenient criterion:

Corollary 3.11. *Let $p \equiv 1 \pmod 6$, $p = a^2 + 3b^2$ with $a \equiv -1 \pmod 3$. Then p is 1-exceptional for $M = 3$ (and $M = 6$) exactly when*

$$(2a)^{p-3}\left((2a)^2 + p\right) \equiv 1 \pmod{p^2}.$$

The next and final result in this section shows that 1-exceptionality is actually the most important case:

Theorem 3.12. *Suppose that $M \geq 2$ and $p \equiv 1 \pmod M$, with $\alpha \geq 2$. If p is α-exceptional, it is also $(\alpha - 1)$-exceptional.*

This means, in particular, that only 1-exceptional primes need to be checked for possible 2-exceptionality. We used the criterion in Corollary 3.10; no new 1-exceptional primes for $M = 3, 6$ were found up to 10^{12}.

Exceptionality criteria that are very similar to Theorem 3.9 and Corollary 3.10 also exist for the case $M = 4$; see Section 4 in [15]. Using this analogue to Corollary 3.10, we searched for 1-exceptional primes (for $M = 4$) up to 10^{11}, but found no new ones. Also, with Theorem 3.12 in mind, we used appropriate criteria to check all entries in Table 2 and found that none are 2-exceptional.

Finally in this section, we remark that the $M = 3$ and $M = 6$ exceptional primes 13, 181, 2521 and 489061 (that is, four of the five listed in Table 2) have the property in common that they satisfy $p^2 = 3x^2 + 3x + 1$ for some integer x. See Section 6 in [10] for this and related results, as well as further comments. It is a further consequence of Theorem 3.9 that all such primes are 1-exceptional, but none are 2-exceptional, for $M = 3$ and $M = 6$.

4. Gauss Factorials of Order 1. Part I

4.1. In this section, which contains our third application of Gauss factorials, we take a somewhat different approach. We fix an integer $M \geq 1$ and ask for which integers n the congruence

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod n, \qquad n \equiv \pm 1 \pmod M, \tag{4. 1}$$

is satisfied. In this section we consider the solutions of (4. 1) in the related cases $M = 3$, $M = 6$. The contents of this section are based on the recent paper [16], where complete proofs, further explanations, and remarks on computations can be found.

Let us first consider the congruence (4. 1) from a more general point of view. The case $M = 1$ is just Theorem 1.2, which gives all solutions. For $M = 2$, see Theorem 1.3 which shows that only 1, 2, and 4 can occur as orders of $\left(\frac{n-1}{2}\right)_n !$ modulo n; the more general case corresponding to (4. 1) was solved in [8]. The case $M = 4$ will be discussed in the next section; see also [14].

Returning to (4. 1), we make the assumption that n has the form

$$\begin{cases} n = p^\alpha w, \quad \text{with} \quad w = q_1^{\beta_1} \dots q_s^{\beta_s} \quad (s \geq 0, \alpha, \beta_1, \dots, \beta_s \in \mathbb{N}), \\ p \equiv 1 \pmod 3, \quad q_1 \equiv \dots \equiv q_s \equiv -1 \pmod 3 \quad \text{distinct primes}, \end{cases} \tag{4. 2}$$

and with the convention that $w = 1$ when $s = 0$. Our main goal is now to characterize integers of this form for which

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad \text{or} \tag{4. 3}$$

$$\left\lfloor \tfrac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}. \tag{4. 4}$$

The first few solutions of each of these congruences are displayed in Table 3.

n (4. 3)	factored	n (4. 4)	factored
26	$2 \cdot \mathbf{13}$	1105	$5 \cdot \mathbf{13} \cdot 17$
244	$2^2 \cdot \mathbf{61}$	14365	$5 \cdot \mathbf{13^2} \cdot 17$
305	$5 \cdot \mathbf{61}$	34765	$5 \cdot 17 \cdot \mathbf{409}$
338	$2 \cdot \mathbf{13^2}$	303535	$5 \cdot 17 \cdot \mathbf{3571}$
9755	$5 \cdot \mathbf{1951}$	309485	$5 \cdot 11 \cdot 17 \cdot \mathbf{331}$
18205	$5 \cdot 11 \cdot \mathbf{331}$	353365	$5 \cdot 29 \cdot \mathbf{2437}$
33076	$2^2 \cdot \mathbf{8269}$	508255	$5 \cdot 11 \cdot \mathbf{9241}$
48775	$5^2 \cdot \mathbf{1951}$	510605	$5 \cdot \mathbf{102121}$
60707	$17 \cdot \mathbf{3571}$	527945	$5 \cdot 11 \cdot 29 \cdot \mathbf{331}$

Table 3: Smallest solutions of (4. 3) and (4. 4); p is in boldface.

At first sight there are no apparent patterns, apart from some factors occurring repeatedly. We also observe that both parts of the table contain integers that are not of the form $1 \pmod 3$, respectively $1 \pmod 6$, which means that in (4. 3) and (4. 4) the floor function is indeed meaningful. Our main results in this section, and the more complete results in the original paper [16], will fully explain the entries in Table 3.

The following examples give a better indication than Table 3 of the challenges and expected results.

Example 2. Let $p = 7$. This is the least possible p in (4. 2). Combining theory and computation we found that there are no solutions of (4. 3) for $s = 0, 1, \ldots, 6$. However, for $s = 7$ we have 27 solutions, between

$n = 7 \cdot 2 \cdot 5 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 531968664833$, and

$n = 7 \cdot 2^9 \cdot 5 \cdot 17 \cdot 353 \cdot 7699649 \cdot 47072139617 \cdot 531968664833$;

these two have, respectively, 30 and 36 decimal digits. On the other hand, (4. 4) has the trivial solution $n = 7$ in the case $s = 0$, and for $s = 1, 2, \ldots, 5$ there are no solutions. For $s = 6$ there is the single 40-digit solution

$$n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$$

As far as the corresponding factors q_j are concerned, we note that $5 \mid 7^2 + 1$, and

$$17 \mid 7^{2^3} + 1 \qquad \text{and} \qquad 169\,553 \mid 7^{2^3} + 1,$$

$$353 \mid 7^{2^4} + 1 \qquad \text{and} \qquad 47\,072\,139\,617 \mid 7^{2^4} + 1,$$

$$7\,699\,649 \mid 7^{2^5} + 1 \qquad \text{and} \qquad 531\,968\,664\,833 \mid 7^{2^5} + 1.$$

We also note that $7^{2^2} + 1$ has no prime factor of the form $q \equiv -1 \pmod 3$; furthermore, the exact power of 2 dividing $(7-1)(7+1)(7^{2^1}+1)\ldots(7^{2^5}+1)$ is 2^9.

Example 3. The next smallest p in (4. 2) is $p = 13$. Again, by combining theoretical results with computations we found that for $s = 0, 1, \ldots, 7$ and 9, the congruence (4. 3) has no solutions. However, for $s = 8$ it has exactly 38 solutions which have between 39 and 43 decimal digits. For reasons of brevity we skip further details, which can be found in [16]. However, we remark that in this example we have solutions of the form (4. 2) with $\alpha = 2$. This happens very rarely; in fact, we will explain later that $p = 13$ is the *only* prime $p < 10^{14}$ which can have $\alpha = 2$; and furthermore, for the same range of primes, (4. 3) or (4. 4) *cannot* have any solutions with $\alpha > 2$.

The fact that $p = 7$ and $p = 13$ both lead to numerous solutions is a bit misleading. In fact, it turns out that there are no solutions of (4. 3) or (4. 4) for $p = 19$, 31, 37, or 43. After these, there are solutions for $p = 61$ and $p = 97$, and then only five more up to 1000. All this leads to the following natural questions:

(i) What determines the presence/absence of solutions?

(ii) What are the factors q_j when solutions exist?

(iii) For what p can solutions exist?

4.2. An explanation of these phenomena is given by the fact that we can find necessary and sufficient conditions for the solutions of

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{n} \quad \text{and} \quad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n !^3 \equiv 1 \pmod{n},$$

i.e., necessary conditions for the original congruences (4. 3) and (4. 4). For greater clarity and simplicity, we restrict ourselves in this exposition to the following special cases:

$$M = 3, \qquad s \geq 2, \qquad w \equiv 1 \pmod{3},$$

where the third condition implies that $n \equiv 1 \pmod{3}$. Our main approach will be to find criteria for

$$\left(\tfrac{n-1}{3}\right)_n !^3 \equiv 1 \pmod{w} \quad \text{and} \tag{4. 5}$$

$$\left(\tfrac{n-1}{3}\right)_n !^3 \equiv 1 \pmod{p^\alpha}, \tag{4. 6}$$

and then to combine the two by way of the Chinese Remainder Theorem.

In order to find congruences modulo w, we define the partial totient function

$$\varphi(M, w) = \#\{\tau \mid 1 \leq \tau \leq \tfrac{w-1}{M}, \gcd(\tau, w) = 1\},$$

which was earlier studied by D. H. Lehmer [27] in a somewhat different form. These objects are used in the following lemma; its proof uses most of what is mentioned in the remainder of this section.

Lemma 4.1. *With n as before, we have*

$$\left(\tfrac{n-1}{3}\right)_n ! \equiv \frac{1}{p^{\varphi(3,w)}} \pmod{w}, \qquad \varphi(3, w) = \tfrac{1}{3}(\varphi(w) + 2^{s-1}). \tag{4. 7}$$

The proof is very technical. The basic idea is to write

$$\tfrac{n-1}{3} = \tfrac{p^\alpha - 1}{3} w + \tfrac{w-1}{3} \qquad (n \equiv 1 \pmod{3}),$$

with a slightly different form when $n \equiv -1 \pmod{3}$. This means that $\lfloor \frac{n-1}{3} \rfloor_n !$ is the product of $\frac{p^\alpha - 1}{3}$ "main terms" and one "remainder term".

By the Gauss-Wilson theorem (1. 9), the main terms mostly evaluate to 1 (mod w). The remainder term is more subtle and requires more care; in addition to the Gauss-Wilson theorem this term also requires the Euler-Fermat theorem for its evaluation. This can actually all be done for arbitrary denominators $M \geq 2$.

To continue, we raise both sides of the congruence in (4. 7) to the 3rd power. We then obtain

$$\left(\tfrac{n-1}{3}\right)_n!^3 \equiv p^{-\varphi(w)-2^{s-1}} \equiv p^{-2^{s-1}} \pmod{w}.$$

Therefore we have

$$\left(\tfrac{n-1}{3}\right)_n!^3 \equiv 1 \pmod{w}$$

exactly when

$$p^{2^{s-1}} - 1 \equiv 0 \pmod{w}.$$

But the left of this factors:

$$p^{2^{s-1}} - 1 = (p-1)(p+1)(p^2+1)\dots(p^{2^{s-2}}+1).$$

We have therefore obtained:

Theorem 4.2. *Let n be as before, with $s \geq 1$. Then* (4. 5) *holds if and only if every $q_i^{\beta_i}$ is a divisor of $p^{2^{s-1}} - 1$; i.e., exactly when every*

$$q_i^{\beta_i} \text{ divides } \begin{cases} p-1, & \text{for } s = 1, \\ (p-1)(p+1)(p^2+1)\dots(p^{2^{s-2}}+1), & \text{for } s \geq 2. \end{cases}$$

We note that this result actually holds for

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n! \equiv 1 \pmod{w},$$

when n is not 1 (mod 3).

4.3. Next we state the second crucial ingredient, which gives the necessary congruences modulo p^α.

Lemma 4.3. *Let $n \equiv 1 \pmod 3$ be as before. Then for $s \geq 2$,*

$$\left(\frac{n-1}{3}\right)_n! \equiv (q_1 \dots q_s)^{(-1)^{s-1}\frac{\varphi(p^\alpha)}{3}} \left(\left(\frac{p^\alpha-1}{3}\right)_p!\right)^{2^s} \pmod{p^\alpha}.$$

Once again, this lemma holds in greater generality, and the proof is again very technical. To apply this lemma, we first observe that by cubing both sides of the congruence, by the Fermat-Euler theorem the term with base $(q_1 \dots q_s)$ becomes 1 (mod p^α). Therefore the congruence (4. 6) is equivalent to

$$(\tfrac{p^\alpha-1}{3})_p!^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha}. \tag{4. 8}$$

We will see that primes p that satisfy this congruence are rather special. Using the same notation as in (3. 1) above, we set

$$\gamma_\alpha^{(3)}(p) := \operatorname{ord}_{p^\alpha}((\tfrac{p^\alpha-1}{3})_p!) \qquad (p \equiv 1 \pmod 3)$$

for the multiplicative order modulo p^α. Then (4. 8) implies

$$\gamma_\alpha^{(3)}(p) = 2^\ell \quad \text{or} \quad 3 \cdot 2^\ell \qquad (0 \leq \ell \leq s). \tag{4. 9}$$

We saw in Section 3 that the sequence $\gamma_1(p), \gamma_2(p), \ldots$ behaves in a very special way. This means, in particular, that (4. 9) implies

$$\gamma_1^{(3)}(p) = 2^\ell \quad \text{or} \quad 3 \cdot 2^\ell.$$

This now gives rise to the following definition:

Definition 4.4. *We call a prime $p \equiv 1 \pmod 3$ a level ℓ Jacobi prime if*

$$\operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 2^\ell \quad \textit{or} \quad \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 3 \cdot 2^\ell.$$

Example 4. For the first three primes $p \equiv 1 \pmod 6$ we find:

$$\begin{aligned} p = 7: &\quad \tfrac{p-1}{3}! = 2, &&\operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 3 = 3 \cdot 2^0; \\ p = 13: &\quad \tfrac{p-1}{3}! = 24, &&\operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 12 = 3 \cdot 2^2; \\ p = 19: &\quad \tfrac{p-1}{3}! = 720, &&\operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 9. \end{aligned}$$

Therefore 7 and 13 are Jacobi of levels 0, resp. 2, while 19 is not Jacobi.

The reason for calling these primes *Jacobi primes* lies in Jacobi's binomial coefficient theorem (Theorem 2.3 above), which has the following easy consequence:

Corollary 4.5. *With p and r as in* (2. 5)*, we have*

$$(\tfrac{p-1}{3})!^3 \equiv \frac{1}{r} \pmod p. \tag{4. 10}$$

As a consequence we get an equivalent definition:

Corollary 4.6. *A prime $p \equiv 1 \pmod 3$ is a level-ℓ Jacobi prime if and only if*

$$\operatorname{ord}_p(r) = 2^\ell.$$

Example 5. For the primes in Example 4 we find:

$$\begin{aligned} p = 7: &\quad 4p = 1^2 + 27 \cdot 1^2, &&\operatorname{ord}_p(1) = 2^0; \\ p = 13: &\quad 4p = (-5)^2 + 27 \cdot 1^2, &&\operatorname{ord}_p(-5) = 2^2; \\ p = 19: &\quad 4p = 7^2 + 27 \cdot 1^2, &&\operatorname{ord}_p(7) = 3. \end{aligned}$$

Once again, we see that 7 and 13 are Jacobi primes, while 19 is not, consistent with Example 4.

Jacobi primes of the lowest levels satisfy some important properties:

Theorem 4.7. (a) *A prime p is a level-0 Jacobi prime exactly when*

$$p = 27X^2 + 27X + 7 \qquad (X \in \mathbb{Z}).$$

(b) *There are no Jacobi primes of level* 1.
(c) *The only level-2 Jacobi prime is $p = 13$.*

Parts (a) and (b) of this result follow easily from Corollary 4.6, while part (c) requires some results from the theory of Pell equations.

Remarks: (1) As expected, level-0 Jacobi primes are quite abundant; the first few (up to 1000) are 7, 61, 331 and 547, and there are a total of 215 105 up to 10^{14}.

(2) On the other hand, there are very few Jacobi primes of levels $\ell \geq 2$. The first few are 13, 97, 193, 409, 769, with a total of only 44 up to 10^{14}.

(3) Because of the substantial differences in their nature (see Theorem 4.7) and in their numbers, we call Jacobi primes of level 0 *standard Jacobi primes*, while Jacobi primes of levels $\ell \geq 2$ will be referred to as *nonstandard Jacobi primes*.

4.4. Finally in this section, we combine the Jacobi prime condition for the congruence (4. 6) to hold (see the development leading up to (4. 9)) with Theorem 4.2. Using a slightly more general setting again, with $n \equiv w \equiv \pm 1 \pmod 3$, we have:

Theorem 4.8. *Let n be as above, with $s \geq 2$ and $\alpha \geq 1$. Then the congruence*

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod n$$

holds exactly when all of the following are satisfied:

(a) *if $\alpha > 1$, then p is $(\alpha - 1)$-exceptional;*

(b) *p is a Jacobi prime of level ℓ for some $0 \leq \ell \leq s$;*

(c) *$q_i^{\beta_i} \mid (p-1)(p+1)(p^2+1)\dots(p^{2^{s-2}}+1)$ for all $1 \leq i \leq s$.*

Note that the condition (a) is vacuous when $\alpha = 1$. Condition (c) is related to factors of generalized Fermat numbers that have Jacobi primes as bases. In fact, the paper [16] (see also the web pages [7]) describes a major computational effort to factor as many of these generalized Fermat numbers as possible.

For the concept of an exceptional prime, see Section 3. Of relevance here is the fact that $p = 13$ is *the only* Jacobi prime $< 10^{14}$ that is also 1-exceptional. Returning to Table 1, we see that $p = 13$ occurs to the power 2; we now know that this is the only prime $< 10^{14}$ with $p \equiv 1 \pmod 3$ with this property.

For numerous further results, examples, computations, tables, and remarks, see the original paper [16] and the web pages [7].

5. Gauss Factorials of Order 1. Part II

In this section we consider one more interesting concept that has not come up earlier. While Section 4 deals mainly with $M = 3$ and $M = 6$, a related development is possible, and has been done, for $M = 4$; see [14]. This is of a similar nature as the $M = 3$ and 6 case, but the details are quite different.

The premise is similar to that of Section 4, and we start with the question: For which $n \equiv 1 \pmod 4$ is the congruence

$$\left(\tfrac{n-1}{4}\right)_n ! \equiv 1 \pmod n \tag{5. 1}$$

satisfied? This is clearly the case for $n = 5$. The next solutions are $n = 205$, 725, 1025, 1105, and there are 37 109 in total up to 10^6. With the exception of $n = 5$ all these moduli have at least two distinct prime factors congruent to $1 \pmod 4$. It would therefore be reasonable to guess that this is always true.

However, it is somewhat surprising that (5. 1) does have solutions with $n \equiv 1 \pmod 4$ and such that n has *just one* prime factor $p \equiv 1 \pmod 4$. It turns out that solutions of this type are extremely rare: only three exist up to 10^{20}; they are shown in Table 4.

n	n factored	p
205479813	$3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
1849318317	$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
233456083377	$3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081$	652081

Table 4: The smallest solutions of (5. 1), $p \equiv 1 \pmod 4$.

The complete characterization of all integers of this kind, some of which are extremely large, is one of the main results of [14]. Apart from the three solutions in Table 4, the next smallest solution we known of has 155 digits. All this is related to the concept of a *Gauss prime*, of which 46817 and 652081 (in Table 4) are examples.

Definition 5.1. *We call a prime $p \equiv 1 \pmod 4$ a Gauss prime of level ℓ if*

$$\operatorname{ord}_p\left(\tfrac{p-1}{4}!\right) = 2^\ell.$$

The name comes from the close connection to Gauss's binomial coefficient theorem, Theorem 1.2. In [14] we explain how Gauss primes can be computed; see Table 5 and the remarks following Theorem 5.3.

ℓ	primes	ℓ	primes
0	5 only	11	120833, 1249520060417
1–3	none	12	12289
4	17, 241, 3361, 46817, 652081, ...	13	1908737, 10812547073
5	97, 257, 929, 262337, 200578817	14	114689, 8780414977
6	193, 65537	16	1179649, 27590657, 2742091777
7	641, 12055618177	18	786433, 3225052512257
8	3200257	24	9273304154113
9	93418448897	35	5841155522561, 54185307406337
10	285697, 345089, 11118593	38	2748779069441

Table 5: Gauss primes $p < 10^{14}$ ($p < 10^{16}$ for $\ell = 5$).

The entries for $0 \le \ell \le 3$ are explained as follows.

Theorem 5.2. *Suppose that $p \equiv 1 \pmod 4$ is a prime. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$.

This theorem says that, apart from $p = 5$, the factorial $\frac{p-1}{4}!$ cannot have orders $1, 2, 4$, or 8. The proof is based on Gauss's Theorem 1.2, together with Corollary 1.1. This result can be extended in different directions; see Corollary 3 and Theorem 5 in [14]. We also note that Theorem 5.2 is similar to parts (b) and (c) of Theorem 4.7. It turns out that Theorem 4.7(a) also has an analogue for Gauss primes:

Theorem 5.3. *A prime $p \equiv 1 \pmod 4$ is a level-4 Gauss prime exactly when $p = p_k := a_{k+1}^2 + a_k^2$ for some $k \ge 1$, with the sequence $\{a_k\}$ defined by $a_0 = 0, a_1 = 1$, and $a_k = 4a_{k-1} - a_{k-2}$.*

It is easily verified that p_k is prime for $1 \le k \le 5$; the corresponding Gauss primes are shown in Table 4 under $\ell = 4$. Using the computer packages Maple and PARI/GP, we obtained the following numerical results:

p_k is composite for $6 \le k \le 100\,000$, except for just 14 values of k, namely 131, 200, 296, 350, 519, 704, 950, 5 598, 6 683, 7 445, 8 775, 8 786, 11 565, 12 483. Using the elliptic curve primality test, François Morain [30] showed that they are all prime. Using again PARI/GP, we also found that for $k = 13\,536$, 18 006, 18 995, 48 773, and 93 344, p_k is a probable prime.

We now return to, and somewhat modify, the original question from the beginning of this section: Suppose we are given

$$n = p^\alpha w, \qquad \text{with} \quad w = q_1^{\beta_1} \cdots q_r^{\beta_r} \quad (r \ge 1), \tag{5. 2}$$

where α, $\beta_1, \ldots, \beta_r$ are positive integers and $p \equiv 1 \pmod 4$ and $q_1 \equiv \ldots \equiv q_r \equiv -1 \pmod 4$ are distinct primes. We then wish to know for which n of this form we have

$$\lfloor \tfrac{n-1}{4} \rfloor_n ! \equiv 1 \pmod n. \tag{5. 3}$$

Even though the left-hand side of (5. 3) is defined for all $n \ge 1$, we restrict ourselves to odd n only, to avoid having too many different cases.

First we state a result that is of a negative nature.

Theorem 5.4. *Let n be as in* (5. 2)*. Then the Gauss factorial $\lfloor \frac{n-1}{4} \rfloor_n !$ cannot have the following orders:*

(a) $1, 2,$ *or* 4 *when* $r = 1$*, except for* $n = 15$*;*
(b) 1 *or* 2 *when* $r = 2$*;*
(c) 1 *when* $r = 3$*.*

This result is best possible; indeed, there are small counterexamples when we have $q_1 \equiv 1 \pmod 4$ in (5. 2). The main result of this section can now be stated as follows.

Theorem 5.5. *Let n be as in* (5. 2)*, with $r \ge 4$. Then* (5. 3) *holds exactly when*

(i) $\operatorname{ord}_{p^\alpha}(\frac{p^\alpha - 1}{4})_p ! = 2^\ell$ *for some* $\ell \ge 4$*,*
(ii) $q_j^{\beta_j} \mid p - 1$ *or* $q_j^{\beta_j} \mid p + 1$ *for* $j = 1, \ldots, r$*,*
(iii) $r \ge \ell$*.*

When $\ell = 4$*, then* (5. 3) *implies* $\alpha = 1$*.*

This result is a direct consequence of a more general theorem; see Theorem 7 in [14]. The proof is of a similar nature as the proof of Theorem 4.8 in that it depends on "explicit formulas", separately modulo p^α and modulo w, and then combined via the Chinese Remainder Theorem. The details, however, are quite different.

It can also be shown that a $p \equiv 1 \pmod 4$ for which Condition (i) in this last theorem holds, necessarily satisfies $\operatorname{ord}_p(\frac{p-1}{4})! = 2^\ell$; that is, p is a level-ℓ Gauss prime.

For further details, including proofs, examples, and remarks concerning computations, see the original paper [14].

6. Conclusion

As already mentioned in Sections 1–5, much more could be said about most of the objects and concepts considered in this exposition, and we refer the reader to the original papers [8]–[16], as well as the web pages [7].

In this expository paper we have tried to exhibit some of the many facets of the Gauss factorial defined by (1. 8), especially as given in the form (1. 10). As we saw in Section 2, and later in Theorem 3.5, quotients of appropriate Gauss factorials can be considered natural extensions of certain binomial coefficients. The strength and unexpected generality of the "Catalan extensions", namely Theorems 2.5, 2.6, and 3.5, can be traced to the close connection between Morita's p-adic gamma function and Gauss factorials. Not surprisingly, then, we obtain strong results in Section 3 in connection with sequences of multiplicative orders and their behaviours, and in particular the exceptions to otherwise very regular patterns.

The concept of multiplicative orders of Gauss factorials of the type (1. 10) was also the main topic of Sections 4 and 5, where in particular we considered the question of characterizing those integers n that give rise to Gauss factorials of order 1 modulo n. This led to special sequences of primes whose corresponding Gauss factorials have powers of 2 as orders. Although we were able to derive many properties of these Jacobi primes (in the cases $M = 3$ and 6) and Gauss primes (in the case $M = 4$), much about them still remains mysterious, and is worthy of further investigation.

Many other open questions remain. Just to name a few, we refer the reader to the summary following (1. 10), and repeat the fact that little is known to us when n does not have a prime factor $\equiv 1 \pmod{M}$. The question raised in the first part of the remark at the end of Section 1 seems less intractable; in fact, some strong patterns emerge in the sequence of all partial products mentioned in that remark. Recall that in this paper we exclusively considered the first of M different partial products.

We encourage the reader to explore these and other questions related to the attractive area of classical number theory surrounding Gauss factorials.

References

[1] T. Agoh, K. Dilcher and L. Skula, *Wilson quotients for composite moduli*, Math. Comp. **67**, (1998) 843–861.

[2] A. Al-Shaghay and K. Dilcher, *Congruences for partial sums of reciprocals*, Fibonacci Quart. **53**, No. 2 (2015) 98–111.

[3] A. Al-Shaghay and K. Dilcher, *Analogues of the binomial coefficient theorems of Gauss and Jacobi*, Int. J. Number Theory **12**, No. 8 (2016) 2125–2145.

[4] F. Beukers, *Arithmetical properties of Picard-Fuchs equations*, Seminaire de théorie des nombres Paris 1982–83. Edited by Marie-José Bertin and Catherine Goldstein. Progress in Mathematics, 51. Birkhäuser, Boston, 1984.

[5] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[6] S. Chowla, B. Dwork and R. Evans, *On the mod p^2 determination of* $\binom{(p-1)/2}{(p-1)/4}$, J. Number Theory **24**, No. 2 (1986) 188–196.

[7] J. B. Cosgrave, *http://www.johnbcosgrave.com/computations.php*

[8] J. B. Cosgrave and K. Dilcher, *Extensions of the Gauss-Wilson theorem*, Integers **8**, (2008) A39; available at http://www.integers-ejcnt.org/vol8.html.

[9] J. B. Cosgrave and K. Dilcher, *Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients*, Acta Arith. **142**, No. 2 (2010) 103–118.

[10] J. B. Cosgrave and K. Dilcher, *The multiplicative orders of certain Gauss factorials*, Int. J. Number Theory **7**, No. 1 (2011) 145–171.
[11] J. B. Cosgrave and K. Dilcher, *An Introduction to Gauss Factorials*, Amer. Math. Monthly **118**, No. 9 (2011) 810–828.
[12] J. B. Cosgrave and K. Dilcher, *Sums of reciprocals modulo composite integers*, J. Number Theory **133**, No. 11 (2013) 3565–3577.
[13] J. B. Cosgrave and K. Dilcher, *On a congruence of Emma Lehmer related to Euler numbers*, Acta Arith. **161**, No. 1 (2013) 47–67.
[14] J. B. Cosgrave and K. Dilcher, *The Gauss-Wilson theorem for quarter-intervals*, Acta Math. Hungar. **142**, No. 1 (2014) 199–230.
[15] J. B. Cosgrave and K. Dilcher, *The multiplicative orders of certain Gauss factorials, II*, Funct. Approx. Comment. Math. **54**, No. 1 (2016) 73–93.
[16] J. B. Cosgrave and K. Dilcher, *A role for generalized Fermat numbers*, Math. Comp. **86**, No. 304 (2017) 899–933.
[17] R. E. Crandall, *Topics in Advanced Scientific Computation*, Springer-Verlag, New York, 1996.
[18] R. Crandall, K. Dilcher and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66**, (1997) 433–499.
[19] L. E. Dickson, *History of the Theory of Numbers. Volume I: Divisibility and Primality*, Chelsea, New York, 1966.
[20] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, edited and supplemented by R. Dedekind, 4th edition, Chelsea Publishing Company, New York, 1968. English translation: Lectures on Number Theory, translated by J. Stillwell, American Mathematical Society, Providence, 1999.
[21] C. F. Gauss, *Disquisitiones Arithmeticae*, Translated and with a preface by Arthur A. Clarke. Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse. Springer-Verlag, New York, 1986. xx+472 pp.
[22] A. Granville, *Arithmetic properties of binomial coefficients I. Binomial coefficients modulo prime powers*, Organic mathematics (Burnaby, BC, 1995), 253–276, CMS Conf. Proc. 20, Amer. Math. Soc. Providence, RI, 1997.
[23] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Oxford University Press, 1979.
[24] R. H. Hudson and K. S. Williams, *Binomial coefficients and Jacobi sums*, Trans. Amer. Math. Soc. **281**, No. 2 (1984) 431–505.
[25] P. Kesava Menon, *A generalization of Wilson's theorem*, J. Indian Math. Soc. (N.S.) **9**, (1945) 79–88.
[26] K. E. Kloss, *Some number theoretic calculations*, J. Res. Nat. Bureau of Stand. B **69**, (1965) 335–339.
[27] D. H. Lehmer, *The distribution of totatives*, Canad. J. Math. **7**, (1955) 347–357.
[28] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. (2) **39**, (1938) 350–360.
[29] Maple, *a computer algebra system*, Available at `http://www.maplesoft.com/products/maple/`.
[30] L. J. Mordell, *The congruence* $(p-1/2)! \equiv \pm 1 \pmod{p}$, Amer. Math. Monthly **68**, (1961) 145–146.
[31] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*. Springer-Verlag, New York, 1979.
[32] S. Sanielevici, *Une généralisation du théorème de Wilson*, Com. Acad. R. P. Romîne **8**, (1958) 737–744.
[33] Š. Schwarz, *The role of semigroups in the elementary theory of numbers*, Math. Slovaca **31**, (1981) 369–395.
[34] Z. H. Sun, *Congruences involving Bernoulli and Euler numbers*, J. Number Theory **128**, (2008) 280–312.
[35] J. Urbanowicz and K. S. Williams, *Congruences for L-functions*, Kluwer Academic Publishers, Dordrecht, 2000.
[36] B. A. Venkov, *Elementary Number Theory*, Wolters-Noordhoff Publishing, Groningen, 1970.