MATHEMATICS OF COMPUTATION
Volume 86, Number 304, March 2017, Pages 899–933
http://dx.doi.org/10.1090/mcom/3111
Article electronically published on April 26, 2016

A ROLE FOR GENERALIZED FERMAT NUMBERS

JOHN B. COSGRAVE AND KARL DILCHER

Abstract. We define a Gauss factorial $N_n!$ to be the product of all positive integers up to N that are relatively prime to $n \in \mathsf{N}$. In this paper we study particular aspects of the Gauss factorials $\lfloor \frac{n-1}{M} \rfloor_n!$ for $M = 3$ and 6, where the case of n having exactly one prime factor of the form $p \equiv 1 \pmod 6$ is of particular interest. A fundamental role is played by those primes $p \equiv 1 \pmod 3$ with the property that the order of $\frac{p-1}{3}!$ modulo p is a power of 2 or 3 times a power of 2; we call them Jacobi primes. Our main results are characterizations of those $n \equiv \pm 1 \pmod M$ of the above form that satisfy $\lfloor \frac{n-1}{M} \rfloor_n! \equiv 1 \pmod n$, $M = 3$ or 6, in terms of Jacobi primes and certain prime factors of generalized Fermat numbers. We also describe the substantial and varied computations used for this paper.

1. Introduction

The Fermat numbers

$$F_k := 2^{2^k} + 1, \qquad k = 0, 1, 2, \ldots,$$

are a well known and intensively studied special number sequence. This is partly due to important applications (e.g., Gauss's construction of a regular n-gon), but also due to the history of this sequence, including Fermat's mistaken claim that all are prime, which was disproved by Euler. It is a well-known fact that no Fermat primes except $F_0, \ldots, F_4$ have been found.

The generalized Fermat numbers, defined for integers $a > b \geq 1$ by

$$F_k(a, b) = a^{2^k} + b^{2^k}, \qquad \gcd(a, b) = 1,\ k = 0, 1, 2, \ldots,$$

were first studied by Euler, who proved a well-known theorem about the structure of their prime factors; see [13, p. 375]. They were then subject to more intensive studies from the 1960s onwards. Among the numerous references for Fermat and generalized Fermat numbers, we mention the books [22,29,30], and [13] for historical references. Of particular interest is the case $b = 1$, namely

$$F_k(a) = a^{2^k} + 1, \qquad k = 0, 1, 2, \ldots. \tag{1.1}$$

These can also be seen as special cases of integers of the form $a^n \pm 1$, whose factorizations have been intensively studied since (at least) the advent of the electronic computer, as part of the "Cunningham Project"; see [3].

Received by the editor July 13, 2015 and, in revised form, August 6, 2015, September 9, 2015, and September 14, 2015.

2010 *Mathematics Subject Classification.* Primary 11A07; Secondary 11B65.

Key words and phrases. Gauss-Wilson theorem, Gauss factorials, congruences, binomial coefficient congruences, generalized Fermat numbers, factors.

This research was supported in part by the NSERC (Canada).

Factorization attempts of such numbers have always tested, and continue to test, the limits of modern factoring and primality testing algorithms, both general and specific to Fermat and related numbers, as well as implementations of these algorithms and the increasingly powerful computer hardware on which they run.

There have been, however, relatively few applications of generalized Fermat numbers; see, e.g., [5, 19, 25–27]. In this paper we present another novel application of the factors of numbers of the type (1.1) for a very special class of bases a.

In Section 2 we state the main objectives of this paper and give a first indication as to how generalized Fermat numbers and their factors will enter. Sections 3–6 contain the main results and proofs, while Section 7 is devoted to computations, including new factors of generalized Fermat numbers. We conclude this paper with some further remarks in Section 8.

2. Gauss factorials

The theorem of Wilson, which states that for a prime p we have $(p-1)! \equiv -1 \pmod{p}$, has a less well-known analogue, due to Gauss, for composite moduli: For any integer $n \geq 2$ we have

$$\prod_{\substack{1\leq j\leq n\\ \gcd(j,n)=1}} j \equiv \begin{cases} -1 \pmod{n} & \text{for} \quad n = 2, 4, p^\alpha, \text{ or } 2p^\alpha, \\ 1 \pmod{n} & \text{otherwise,} \end{cases} \tag{2.1}$$

where p is an odd prime and α is a positive integer. For references, see [13, p. 65].

With this theorem in mind, we have used the term *Gauss factorial* in previous papers (see, e.g., [9]) to refer to the factorial-like product

$$N_n! = \prod_{\substack{1\leq j\leq N\\ \gcd(j,n)=1}} j, \qquad N, n \in \mathsf{N}. \tag{2.2}$$

Such products play an important role in number theory, for instance in the definition of Morita's p-adic Gamma function (see, e.g., [2, p. 227]).

In this paper we continue our study of the arithmetic properties of the Gauss factorial $\lfloor \frac{n-1}{M} \rfloor_n!$, $M \geq 1$, $n \equiv \pm 1 \pmod{M}$. In particular, given a fixed integer $M \geq 1$ we consider the question of which integers n satisfy

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}. \tag{2.3}$$

More general questions on the residues or the multiplicative orders modulo n of the Gauss factorials in (2.3) can also be (and have been) considered. However, it is the purpose of this paper to study the solutions of (2.3) in the two closely related cases $M = 3$ and $M = 6$.

We begin by putting the congruence (2.3) in perspective. When $M = 1$, this is just the Gauss-Wilson theorem, and all solutions are given by (2.1). The case $M = 2$ was completely solved in [7], where it was shown that the only possible orders of $\left(\frac{n-1}{2}\right)_n!$ modulo n are 1, 2, and 4. The case $M = 4$ was considered in [10], where the methods and results were similar in nature to the present paper, with some substantial differences, however.

Another way of characterizing the Gauss factorials in (2.3) is by the number of distinct prime factors $p \mid n$ for which $p \equiv 1 \pmod{M}$. If n has at least three such prime factors, then (2.3) always holds for $n \equiv 1 \pmod{M}$, as was shown in [7], and an easy extension of the proof given in [7] establishes the same result in the

case where $n \equiv -1 \pmod{M}$. If n has exactly two distinct prime factors $p \equiv 1 \pmod{M}$, the situation becomes more interesting, and a typical result is given as an illustration in Subsection 8.3 at the end of this paper.

Of the two remaining cases, very little can be said when n has no prime factor of this kind. However, when n has exactly one such prime factor, a very rich structure and strong and pleasing results emerge; this case was already explored in [8] and [11] when n is a prime power.

Let us now make the question around (2.3) more specific. From here on we always assume that n is of the form

$$\begin{cases} n = p^\alpha w, \quad \text{with} \quad w = q_1^{\beta_1} \dots q_s^{\beta_s} \quad (s \geq 0, \alpha, \beta_1, \dots, \beta_s \in \mathsf{N}), \\ p \equiv 1 \pmod 3, \quad q_1 \equiv \dots \equiv q_s \equiv -1 \pmod 3 \quad \text{distinct primes}, \end{cases} \tag{2.4}$$

where the case $s = 0$ is interpreted as $w = 1$. The main objective of this paper is to study integers of this type for which

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod n \qquad \text{or} \tag{2.5}$$

$$\left\lfloor \tfrac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod n. \tag{2.6}$$

Table 2.1 shows the first few solutions of each of these two congruences.

TABLE 2.1. The first solutions of (2.5) and (2.6); p shown in bold.

n (2.5)	factored	n (2.6)	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	$5 \cdot 11 \cdot 29 \cdot \mathbf{331}$

While no strong patterns appear in this table, we observe that both tables contain integers n that are not 1 (mod 3), resp. 1 (mod 6), so that the floor functions in (2.5) and (2.6) are indeed meaningful. All entries in Table 2.1 can be completely explained by our main results later in this paper.

In the process of studying the solutions of these two congruences (2.5) and (2.6), we prove more general results, and we encounter phenomena that are interesting in their own right. But first we continue with two motivating examples.

Example 2.2. Let $p = 7$, the smallest admissible p in (2.4). A combination of theory and computation establishes that for $s = 0, 1, \dots, 6$ there are no solutions of (2.5), while for $s = 7$ there are exactly 27 solutions, the smallest and largest of which are

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

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

with 30 and 36 decimal digits, respectively. As far as (2.6) is concerned, we have the trivial solution $n = 7$ for $s = 0$, while there are no solutions for $s = 1, 2, \dots, 5$,

and a single one for $s = 6$, namely the 40-digit solution

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

What are these factors q_j that occur in these cases? We note that $5 \mid 7^2 + 1$, and

$$17 \mid 7^{2^3} + 1 \qquad \text{and} \qquad 169\,553 \mid 7^{2^3} + 1,$$
$$353 \mid 7^{2^4} + 1 \qquad \text{and} \qquad 47\,072\,139\,617 \mid 7^{2^4} + 1,$$
$$7\,699\,649 \mid 7^{2^5} + 1 \qquad \text{and} \qquad 531\,968\,664\,833 \mid 7^{2^5} + 1,$$

while $7^{2^2} + 1$ has no prime factor $q \equiv -1 \pmod 3$, and 2^9 is the exact power of 2 that divides $(7-1)(7+1)(7^{2^1}+1)\dots(7^{2^5}+1)$.

Example 2.3. Let $p = 13$, the next admissible p in (2.4). Again, a combination of theory and computation establishes that (2.5) has no solution for $s = 0, 1, \dots, 7$ and 9, while there are exactly 38 solutions for $s = 8$, the smallest and largest of which have 39 and 43 digits, respectively. Those solutions are as follows (with $\alpha = 1, 2$ and $\beta = 1, 2, \dots, 9$):

$13^\alpha \cdot 2^\beta \cdot 5 \cdot 17 \cdot 257 \cdot 2657 \cdot 10433 \cdot 441281 \cdot 36713826768408543617$,
$13^\alpha \cdot 2^\beta \cdot 5 \cdot 17 \cdot 1601 \cdot 2657 \cdot 10433 \cdot 441281 \cdot 36713826768408543617$,
$13^\alpha \cdot 5 \cdot 17 \cdot 257 \cdot 1601 \cdot 2657 \cdot 10433 \cdot 441281 \cdot 36713826768408543617$.

On the other hand, a combination of theory and computation also establishes that (2.6) has no solution for $s = 0, 1$, and exactly two solutions for $s = 2$, namely 1105 and 14365: $13^\alpha \cdot 5 \cdot 17$ ($\alpha = 1, 2$).

Further, there are no solutions for $s = 3, 4, 5, 6$ and 8, while there are exactly eight solutions for $s = 7$, the smallest and largest of which have 22 and 43 digits, respectively. Those solutions are as follows (for $\alpha = 1, 2$):

$13^\alpha \cdot 5 \cdot 17 \cdot 257 \cdot 1601 \cdot 2657 \cdot 10433 \cdot 441281$,
$13^\alpha \cdot 5 \cdot 17 \cdot 257 \cdot 1601 \cdot 2657 \cdot 10433 \cdot 36713826768408543617$,
$13^\alpha \cdot 5 \cdot 17 \cdot 257 \cdot 1601 \cdot 2657 \cdot 441281 \cdot 36713826768408543617$,
$13^\alpha \cdot 5 \cdot 257 \cdot 1601 \cdot 2657 \cdot 10433 \cdot 441281 \cdot 36713826768408543617$.

In the case of the solutions to (2.5), the prime powers occurring in the construction of the factor w in (2.4) (up to $s = 8$) are divisors of the product

$$(13-1)(13+1)(13^{2^1}+1)\dots(13^{2^6}+1), \tag{2.7}$$

where the exponent 6 comes from $s - 2$. In the case of the solutions to (2.6), the prime powers (up to $s = 7$) are divisors of the same product (2.7), but this time the exponent 6 comes from $s - 1$. Since we have complete factorizations of the generalized Fermat numbers in (2.7), we can be certain that the solutions displayed in this example are complete up to $s = 8$, resp. $s = 7$, as we will see later.

Remark 2.4. In Example 2.3 we have solutions of the form (2.4) with $\alpha = 2$. This is an extremely rare event; in fact, as will be explained later, $p = 13$ is the only prime $p < 10^{14}$ for which $\alpha = 2$ can occur. We will also show that there cannot be any solutions with $\alpha > 2$ for p in the same range.

Having displayed numerous solutions for $p = 7$ and 13 in Examples 2.2 and 2.3, we note that as a consequence of the theory developed in this paper, there are no solutions of either (2.5) or (2.6) for $p = 19$, 31, 37, or 43, with the next solutions occurring for $p = 61$ and $p = 97$, and only five more such p below 1000.

In this paper we will give a complete characterization of these special primes 7, 13, 61, 97, ..., which we call *Jacobi primes*, and also explain and characterize the structure of the solutions of (2.5) and (2.6), as seen in Examples 2.2 and 2.3. Key ingredients to all of this are closed form congruences, split modulo p^α and modulo w, which will be stated in the following section.

3. Closed form congruences

The proofs of our main results in Section 5, and thus the solutions to the congruences (2.5) and (2.6), depend on certain explicit congruences modulo p^α, and separately modulo w, where $n = p^\alpha w$ as in (2.4). In this section we will state these congruences; later, in Section 5, they will be combined by using the Chinese Remainder Theorem.

3.1. **Congruences modulo w.** We require the following definitions, partially modified from D. H. Lehmer's paper [23]. As usual, $\varphi(n)$ denotes Euler's totient function. For positive integers $k < n$ we define, for each $q = 1, 2, \ldots, k$, the partial totient function $\varphi(k, q, n)$ as the number of totatives τ, that is, integers τ relatively prime to n, for which

$$\frac{n(q-1)}{k} < \tau < \frac{nq}{k}.$$

Here we will be dealing with the special cases

$$\varphi(M, 1, w) = \#\{\tau \mid 1 \le \tau \le \tfrac{w-1}{M}, \gcd(\tau, w) = 1\}. \tag{3.1}$$

With this definition we can now state the following two lemmas. Their proofs lie at the centre of most of this paper, but for the sake of greater clarity of exposition we defer them to Section 6.

Lemma 3.1. *Let n be as in* (2.4)*, with $w \equiv \delta \pmod 3$, where $\delta \in \{-1, 1\}$. Then*

$$\lfloor \tfrac{n-1}{3} \rfloor_n ! \equiv \frac{1}{p^{\varphi(3,1,w)}} \pmod w, \qquad \varphi(3, 1, w) = \frac{1}{3}\left(\varphi(w) + \delta 2^{s-1}\right). \tag{3.2}$$

Lemma 3.2. *Let n be as in* (2.4)*, with $w \equiv \delta \pmod 6$, where $\delta \in \{-1, 1\}$. Then*

$$\lfloor \tfrac{n-1}{6} \rfloor_n ! \equiv \frac{B_s(n)}{p^{\varphi(6,1,w)}} \pmod w, \qquad \varphi(6, 1, w) = \frac{1}{6}\left(\varphi(w) + \delta 2^{s+1}\right), \tag{3.3}$$

with

$$B_s(n) = \begin{cases} (-1)^{(p-1)/6}, & s = 1, \\ 1, & s \ge 2. \end{cases}$$

We note that the right-hand sides of (3.2) and (3.3) are independent of α, the exponent of p in (2.4). Before stating the closed-form congruences modulo p^α, we derive some consequences from Lemmas 3.1 and 3.2, which will already show how generalized Fermat numbers enter the picture. For the proof of the first consequence we require the following lemma.

Lemma 3.3. *For w as in* (2.4)*, the congruence $X \equiv 1 \pmod w$ holds if and only if $X^3 \equiv 1 \pmod w$ holds.*

Proof. The first congruence obviously implies the second one. Suppose now that $X^3 \equiv 1 \pmod w$; then $(X-1)(X^2+X+1) \equiv 0 \pmod w$. But $X^2 + X + 1 \equiv 0 \pmod q$ if and only if $(2X+1)^2 \equiv -3 \pmod q$, which is impossible for

primes $q \equiv -1 \pmod 3$ since -3 is a quadratic nonresidue for such primes. Hence $\gcd(w, X^2+X+1) = 1$ for any $X \in \mathsf{Z}$, so $w \mid X-1$, which completes the proof. ▫

Proposition 3.4. *Let n be as in (2.4), with $s \ge 1$. Then*

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod w \tag{3.4}$$

if and only if every $q_i^{\beta_i}$ is a divisor of $p^{2^{s-1}} - 1$; in other words, if and only if every

$$q_i^{\beta_i} \text{ divides } \begin{cases} p-1, & \text{for } s = 1, \\ (p-1)(p+1), & \text{for } s = 2, \\ (p-1)(p+1)(p^2+1)\dots(p^{2^{s-2}}+1), & \text{for } s \ge 3. \end{cases}$$

Proof. Raise both sides of (3.2) to the third power. Then we get

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv p^{-\varphi(w)-\delta 2^{s-1}} \equiv p^{-\delta 2^{s-1}} \pmod w, \qquad \delta = \pm 1.$$

By Lemma 3.3 we now have (3.4) if and only if $p^{2^{s-1}} \equiv 1 \pmod w$, which was to be shown. ▫

In a completely analogous way we may obtain the following result from (3.3).

Proposition 3.5. *Let the odd integer n be as in (2.4), with $s \ge 2$. Then*

$$\left\lfloor \tfrac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod w \tag{3.5}$$

if and only if every $q_i^{\beta_i}$ is a divisor of $p^{2^s} - 1$; in other words, if and only if

$$q_i^{\beta_i} \Big| (p-1)(p+1)(p^2+1)\dots(p^{2^{s-1}}+1), \quad \text{for all } i = 1, \dots, s.$$

The condition $s \ge 2$ is necessary in this result because of the term $B_s(n)$ in (3.3). Also, the proof would use the easily derivable congruence $p^{\varphi(w)/2} \equiv 1 \pmod w$, which holds for $s \ge 2$.

Example 3.6. Let $p = 19$. We compute

$$p-1 = 2 \cdot 3^2, \quad p+1 = 2^2 \cdot 5, \quad p^{2^1}+1 = 2 \cdot 181, \quad p^{2^2}+1 = 2 \cdot 17 \cdot 3833,$$

and we note that among these factors, $q_1 = 5$, $q_2 = 17$, and $q_3 = 3833$ satisfy $q_i \equiv -1 \pmod 6$. Hence for $s = 3$ the hypotheses of Proposition 3.5 are satisfied, and $n = 19^\alpha w$ with $w = 5 \cdot 17 \cdot 3833$ is a solution of (3.5).

On the other hand, there can be no solution for $s = 2$ since $q_1 = 5$ is the only admissible prime factor up to the appropriate level. Also, it is important to note that the above n is *not* a solution of (2.6). For this to be the case, we would need $\left\lfloor \tfrac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{p^\alpha}$, which cannot hold, as we shall see later.

The reader will have noticed that, in contrast to Proposition 3.4, the case $s = 1$ is not mentioned in Proposition 3.5 or in Example 3.6. This case needs to be treated separately.

Proposition 3.7. *Let $n = p^\alpha q^\beta$ with primes $p \equiv 1 \pmod 6$, $q \equiv -1 \pmod 6$ and $\alpha, \beta \ge 1$. Then*

$$\left\lfloor \tfrac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{q^\beta} \tag{3.6}$$

if and only if $q^\beta \mid p^2 - (\frac{p}{q})(-1)^{(p-1)/2}$, where $(\frac{p}{q})$ is the Legendre symbol. In other words, (3.6) holds if and only if $q^\beta \mid (p-1)(p+1)$ or $q^\beta \mid p^2+1$, depending on whether $(\frac{p}{q})(-1)^{(p-1)/2} = 1$ or -1.

Proof. By Lemma 3.3 we know that (3.6) holds if and only if the cube of this congruence holds. By (3.3) this is the case when

$$p^{\frac{1}{2}\varphi(q^\beta)+2\delta} \equiv (-1)^{(p-1)/2} \pmod{q^\beta}. \tag{3.7}$$

But by the theory of quadratic residues (using Euler's criterion) we have

$$p^{\frac{1}{2}\varphi(q^\beta)} \equiv (\frac{p}{q}) \pmod{q^\beta}.$$

Since the Legendre symbol and the right-hand side of (3.7) are 1 or -1, the exponent $\delta = \pm 1$ is irrelevant, and (3.7) is now seen to be equivalent to $p^2 \equiv (\frac{p}{q})(-1)^{(p-1)/2} \pmod{q^\beta}$, which was to be shown. □

We illustrate this result with two examples.

Example 3.8. Let $p = 349$ and $q = 5$. Then $(\frac{p}{q})(-1)^{(p-1)/2} = 1 \cdot 1 = 1$. So we consider $(p-1)(p+1) = 348 \cdot 350 = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 29$, and by Proposition 3.7 the congruence (3.6) holds for $n = 349^\alpha \cdot 5^2$ for any $\alpha \geq 1$. For instance, for $\alpha = 2$ we compute

$$\lfloor \tfrac{n-1}{6} \rfloor_n ! \equiv 596726 \pmod{n} \equiv 1 \pmod{5^2}.$$

Example 3.9. Let $p = 463$ and $q = 17$. Then $(\frac{p}{q})(-1)^{(p-1)/2} = 1 \cdot (-1) = -1$. So this time we consider $p^2 + 1 = 2 \cdot 5 \cdot 13 \cdot 17 \cdot 97$, and by Proposition 3,7 we know that (3.6) holds for $n = 463^\alpha \cdot 17$ for any $\alpha \geq 1$. We choose again $\alpha = 2$ and compute

$$\lfloor \tfrac{n-1}{6} \rfloor_n ! \equiv 994637 \pmod{n} \equiv 1 \pmod{17}.$$

3.2. **Congruences modulo p^α.** The following two lemmas contain a second set of crucial closed-form congruences for denominators $M = 3$ and $M = 6$, respectively. Their proofs will also be presented in Section 6.

Lemma 3.10. *Let $n \equiv \delta \pmod 3$, $\delta \in \{-1, 1\}$, be as in (2.4). Then for $s \geq 1$,*

$$\lfloor \tfrac{n-1}{3} \rfloor_n ! \equiv \varepsilon(n)(q_1 \dots q_s)^{(-1)^{s-1}\delta\varphi(p^\alpha)/3} (\tfrac{p^\alpha - 1}{3})_p !^{\delta 2^s} \pmod{p^\alpha}, \tag{3.8}$$

where

$$\varepsilon(n) := \begin{cases} -1 & \text{when } s = 1 \text{ with } q_1 = 2 \text{ and } \beta_1 = 1, \\ 1 & \text{otherwise.} \end{cases}$$

Lemma 3.11. *Let $n \equiv \delta \pmod 6$, $\delta \in \{-1, 1\}$, be as in (2.4). Then we have*

$$\lfloor \tfrac{n-1}{6} \rfloor_n ! \equiv (-1)^{(p+q_1)/6} q_1^{\delta\varphi(p^\alpha)/6} (\tfrac{p^\alpha - 1}{6})_p !^{2\delta} \pmod{p^\alpha} \quad (s = 1), \tag{3.9}$$

$$\lfloor \tfrac{n-1}{6} \rfloor_n ! \equiv (q_1 \dots q_s)^{(-1)^s \delta\varphi(p^\alpha)/3} (\tfrac{p^\alpha - 1}{6})_p !^{\delta 2^s} \pmod{p^\alpha} \quad (s \geq 2). \tag{3.10}$$

We note that the right-hand sides of (3.8)–(3.10) are independent of the powers of $q_1, \dots, q_s$. While the main purpose of this paper is to study solutions of the congruences (2.5) and (2.6), Examples 2.2 and 2.3 suggest that the Gauss factorials $\lfloor \frac{n-1}{3} \rfloor_n !$ and $\lfloor \frac{n-1}{6} \rfloor_n !$ are closely related to each other. As another application of the closed-form congruences stated above we will now make this connection more explicit.

Proposition 3.12. *Let n be as in (2.4), with $q_j \equiv -1 \pmod 6, j = 1, \dots, s$. Then*

$$\lfloor \tfrac{n-1}{3} \rfloor_n !^{24} \equiv \lfloor \tfrac{n-1}{6} \rfloor_n !^{12} \pmod{n} \quad \text{when } s = 0, \tag{3.11}$$

$$\lfloor \tfrac{n-1}{3} \rfloor_n !^{12} \equiv \lfloor \tfrac{n-1}{6} \rfloor_n !^{6} \pmod{n} \quad \text{when } s = 1, \tag{3.12}$$

$$\lfloor \tfrac{n-1}{3} \rfloor_n !^{6} \equiv \lfloor \tfrac{n-1}{6} \rfloor_n !^{3} \pmod{n} \quad \text{when } s \geq 2. \tag{3.13}$$

Proof. The case $s = 0$ is Corollary 1 in [11]. Next, for $s = 1$ we raise both sides of (3.8) and (3.9) to the twelfth and sixth powers, respectively. Then by the Euler-Fermat theorem all but the last term on each of the right-hand sides become 1, and using the case $s = 0$ gives

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^{12} \equiv \left\lfloor \tfrac{n-1}{6} \right\rfloor_n !^{6} \pmod{p^\alpha}. \tag{3.14}$$

Now, raising (3.2) and (3.3) to the same powers, we get

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^{12} \equiv p^{-4\varphi(w)-\delta 2^{s+1}} \pmod{w}, \quad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n !^{6} \equiv p^{-\varphi(w)-\delta 2^{s+1}} \pmod{w}.$$

Since $p^{\varphi(w)} \equiv 1 \pmod{w}$, the left terms in the above two congruences are congruent to each other modulo w. Combining this with (3.14) by using the Chinese Remainder Theorem gives (3.12).

Finally, in the case $s \geq 2$ we raise (3.8) and (3.10) to the sixth and third powers, respectively, and once again use the case $s = 0$. This gives

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^{6} \equiv \left\lfloor \tfrac{n-1}{6} \right\rfloor_n !^{3} \pmod{p^\alpha}. \tag{3.15}$$

Just as before, (3.2) and (3.3) give

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^{6} \equiv p^{-2\varphi(w)-\delta 2^{s}} \pmod{w}, \quad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n !^{3} \equiv p^{-\varphi(w)/2-\delta 2^{s}} \pmod{w}.$$

Once again, we have $p^{\varphi(w)} \equiv 1 \pmod{w}$, and $p^{\varphi(w)/2} \equiv 1 \pmod{w}$, since $s \geq 2$. So the terms on the left-hand sides above are congruent to each other modulo w, and combining this with (3.15), the Chinese Remainder Theorem gives (3.13), and the proof is complete. □

Remark 3.13. Examples show that the exponents in each of the three cases in Proposition 3.12 are best possible.

4. Jacobi primes

4.1. **Basics.** We will now use the closed-form congruences from the previous section to motivate the main definition in the current section; this is also a central concept for this paper. For this purpose, and to simplify matters, we restrict our attention to integers of the form (2.4) with $s \geq 2$ and to the case of the congruence (2.5). A necessary condition for this congruence to hold is that the third power also holds. We therefore cube both sides of (3.8), which shows that a necessary condition for (2.5) to hold is that

$$(\tfrac{p^\alpha-1}{3})_p !^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha} \tag{4.1}$$

be satisfied. We will see later that this congruence places an extremely strong condition on the prime p whenever $\alpha > 1$. But first we will see that for any $\alpha \geq 1$ the primes p that satisfy (4.1) are rather special. Using the notation

$$\gamma_\alpha^{(M)}(p) := \operatorname{ord}_{p^\alpha}((\tfrac{p^\alpha-1}{M})_p !) \qquad (M \geq 2,\ p \equiv 1 \pmod{M}) \tag{4.2}$$

for the multiplicative order modulo p^α, the congruence (4.1) implies that

$$\gamma_\alpha^{(3)}(p) = 2^\ell \quad \text{or} \quad 3 \cdot 2^\ell \qquad (0 \leq \ell \leq s). \tag{4.3}$$

Now, in Proposition 4.2 of [8] it was shown that the sequence of orders $\gamma_1^{(M)}(p)$, $\gamma_2^{(M)}(p), \ldots$ behaves in a very specific way, which in the above situation means that (4.3) implies

$$\gamma_1^{(3)}(p) = \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 2^\ell \quad \text{or} \quad 3 \cdot 2^\ell. \tag{4.4}$$

This gives rise to the following definition.

Definition 4.1. A prime $p \equiv 1 \pmod 3$ will be called a Jacobi prime of level ℓ if

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

Example 4.2. We consider the first three primes $p \equiv 1 \pmod 6$ and compute:

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

Thus, 7 and 13 are Jacobi primes of levels 0 and 2, respectively, while 19 is not a Jacobi prime.

An equivalent definition given below is related to another important ingredient in our eventual characterization of the solutions of (2.5) and (2.6), namely Jacobi's binomial coefficient congruence.

Theorem 4.3 (Jacobi)**.** *Let $p \equiv 1 \pmod 3$, and write*

$$4p = r^2 + 27t^2, \quad r \equiv 1 \pmod 3, \tag{4.5}$$

which uniquely determines the integer r. Then

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p. \tag{4.6}$$

This remarkable result is nonelementary, and a proof can be found in [2], the standard reference in the field. For remarks and further references, see [2, p. 291]. As an easy consequence of Jacobi's theorem we obtain the following congruence.

Corollary 4.4. *Let p and r be as in* (4.5)*. Then*

$$(\tfrac{p-1}{3})!^3 \equiv \frac{1}{r} \pmod p. \tag{4.7}$$

Proof. We rewrite (4.6) as

$$(\tfrac{2(p-1)}{3})! \equiv -r(\tfrac{p-1}{3})!^2 \pmod p. \tag{4.8}$$

Since $\frac{p-1}{3}$ is even, we have $(\frac{p-1}{3})! \equiv (p-1)(p-2)\dots(p-\frac{p-1}{3}) \pmod p$ and therefore, upon multiplying both sides of (4.8) by $(\frac{p-1}{3})!$, the left-hand side becomes $(p-1)! \equiv -1 \pmod p$, by Wilson's theorem; (4.7) now follows immediately. ▫

Corollary 4.4 shows that we have the equivalence

$$(\tfrac{p-1}{3})!^{3\cdot 2^m} \equiv 1 \pmod p \quad \Leftrightarrow \quad r^{2^m} \equiv 1 \pmod p \quad (m \geq 0),$$

and by (4.4) we get the following equivalent to Definition 4.1.

Corollary 4.5. *A prime $p \equiv 1 \pmod 3$ is a Jacobi prime of level ℓ if and only if*

$$\operatorname{ord}_p(r) = 2^\ell, \tag{4.9}$$

where r is as defined in (4.5)*.*

Example 4.6. We consider again the primes of Example 4.2 and compute:

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

By Corollary 4.5, this is consistent with Example 4.2.

We will see later that it is Corollary 4.5 rather than Definition 4.1 that allows for the most efficient computation of Jacobi primes. But first we derive some important conditions for levels 0, 1 and 2.

Proposition 4.7. (a) *A prime p is a level-0 Jacobi prime if and only if*

$$p = 27X^2 + 27X + 7 \qquad (X \in \mathsf{Z}). \tag{4.10}$$

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

Proof. (a) By Corollary 4.5, p is a level-0 Jacobi prime if and only if $r = 1$, which by (4.5) means that $4p = 1 + 27t^2 = 1 + 27(2X + 1)^2$, where we used the fact that t must be odd. Upon expanding and dividing by 4, we immediately get (4.10).

(b) Again by Corollary 4.5, p is of level 1 if and only if $r \equiv -1 \pmod p$. The case $r = -1$ is a contradiction to $r \equiv 1 \pmod 3$. By (4.5) we have the restriction $|r| < 2\sqrt{p}$, an inequality not satisfied by the next-smallest r, namely $r = p - 1$, since $p \geq 7$. This proves part (b).

(c) In this case we have $\operatorname{ord}_p(r) = 4$, i.e., $r^2 \equiv -1 \pmod p$. Due to the size restriction $|r| < 2\sqrt{p}$ from above, r^2 has to be of the form $r^2 + 1 = mp$, $1 \leq m \leq 4$. Since $r^2 + 1 \equiv 2 \pmod 3$, the cases $m = 1$, 3 and 4 lead to contradictions to $p \equiv 1 \pmod 3$. This leaves $m = 2$, and we wish to show that $2p = r^2 + 1$ implies $p = 13$. To do so, we combine this identity with (4.5), obtaining

$$r^2 - 27t^2 = -2 \quad \text{or} \quad x^2 - 3y^2 = -2.$$

Without going into details, we now appeal to the theory of Pell equations. Let (x_k, y_k) be the solutions of $x^2 - 3y^2 = -2$, and (A_k, B_k) the solutions of $x^2 - 3y^2 = 1$. All four sequences, with numerous properties and references, can be found in [28] as A001834, A001835, A001075 and A00353, respectively. The one property we require here is that $x_k^2 + 1 = A_{2k-1}$, which can be verified, for instance, by manipulating the relevant Binet-type formulas. This identity implies, with the above, that a level-2 Jacobi prime p satisfies $2p = r^2 + 1 = x_k^2 + 1 = A_{2k-1}$. $A_3 = 26$ is one such solution. But as far as other solutions are concerned, it was shown in [8, Lemmas 7–9] that for no other case can we have $r^4 \equiv 1 \pmod 4$, a contradiction to the level of p being 2. Hence $p = 13$ is the only level-2 Jacobi prime. ∎

Remark 4.8. (1) As one would expect, (4.10) generates a large number of primes, although it is not known whether there are infinitely many. The first few (up to 1000) are 7, 61, 331 and 547, with the total of 215 105 such primes up to 10^{14}. On the other hand, Jacobi primes of levels $\ell \geq 3$ are very rare, with only 44 up to 10^{14}; see Section 7 for a complete list.

(2) Because of this large difference in their abundance, we shall refer to level-0 Jacobi primes as *standard*, and those of levels $\ell \geq 2$ as *nonstandard Jacobi primes*.

(3) For a standard Jacobi prime p, (4.10) gives an explicit representation $p = a^2 + 3b^2$. Indeed, it is easy to verify that

$$p = \left(\tfrac{9X+4}{2}\right)^2 + 3\left(\tfrac{3X+2}{2}\right)^2 \ (X \text{ even}) \quad \text{or} \quad p = \left(\tfrac{9X+5}{2}\right)^2 + 3\left(\tfrac{3X+1}{2}\right)^2 \ (X \text{ odd}).$$

This also shows that $b \equiv 1 \pmod 3$, resp. $b \equiv 2 \pmod 3$, and in particular b is never divisible by 3. For Jacobi primes of level $\ell \geq 2$ there is no obvious way to determine a and b, other than the usual algorithms.

4.2. **The "denominator 6" case.** This is the case of solutions of (2.6), where once again we assume $s \geq 2$ for simplicity. In analogy to the development at the beginning of this section we see that a necessary condition for (2.6) to hold is that

$$(\tfrac{p^\alpha-1}{6})_p!^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha} \tag{4.11}$$

be satisfied, which, again using the theory developed in [8], requires that

$$\gamma_1^{(6)}(p) = \operatorname{ord}_p\left(\tfrac{p-1}{6}!\right) = 2^L \quad \text{or} \quad 3\cdot 2^L \qquad (0 \leq L \leq s). \tag{4.12}$$

We will now see that such a prime p also has to be a Jacobi prime whose level ℓ is closely related to L. First we require another binomial coefficient congruence, similar in nature to Jacobi's theorem.

Given a prime $p \equiv 1 \pmod 6$, by a result going back to Fermat it can be written as $p = a^2 + 3b^2$, uniquely up to signs of a and b. It was Jacobi who used the alternative representation $4p = x^2 + 3y^2$ and showed that it always has three distinct solutions (up to sign) that can be written in terms of a and b. For an exposition of this, with references and a table of small primes, see [9].

One of the three representations is given by (4.5), and below we write r in terms of a and b. We also need an integer u satisfying $4p = u^2 + 3v^2$ which is written in terms of a and b in a similar way.

Let $p = a^2 + 3b^2$ with the signs chosen so that $a \equiv -1 \pmod 3$ and $b > 0$; then we define u by the following congruences modulo p, with r given as comparison:

$$u \equiv \begin{cases} 2a & \text{if} \quad b \equiv 0 \pmod 3, \\ -a-3b & \text{if} \quad b \equiv 1 \pmod 3, \\ -a+3b & \text{if} \quad b \equiv 2 \pmod 3; \end{cases} \quad r \equiv \begin{cases} 2a & \text{if} \quad b \equiv 0 \pmod 3, \\ -a+3b & \text{if} \quad b \equiv 1 \pmod 3, \\ -a-3b & \text{if} \quad b \equiv 2 \pmod 3. \end{cases} \tag{4.13}$$

For r these are actually equations for all $p \equiv 1 \pmod 6$, while for u they hold as equations for $p \geq 19$, with $u = -5$ when $p = 7$ and $u = 7$ when $p = 13$.

Before continuing, we use these congruences to obtain a simple but useful connection between r and u, which was also proved in [11, Lemma 3].

Lemma 4.9. *For any $p \equiv 1 \pmod 6$ we have $r^3 \equiv u^3 \pmod p$.*

Proof. We consider the factorization $r^3 - u^3 = (r-u)(r^2 + ru + u^2)$ and use the fact that $r = u$ when $b \equiv 0 \pmod 3$. When $b \equiv \pm 1 \pmod 3$ then in both cases,

$$r^2+ru+u^2 \equiv (a+3b)^2+(a+3b)(a-3b)+(a-3b)^2 = 3(a^2+3b^2) = 3p \equiv 0 \pmod p,$$

so in all three cases we have $r^3 - u^3 \equiv 0 \pmod p$. ∎

We now state the following congruence, which is similar in nature to Jacobi's theorem and which was proved in [21]; see also [2, p. 270].

Theorem 4.10 (Hudson and Williams)**.** *Let $p \equiv 1 \pmod 6$ be a prime and u as defined above. Then*

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1} u \pmod p. \tag{4.14}$$

We can now state and prove the following result related to (4.12).

Proposition 4.11. *Let p be a Jacobi prime of level $\ell \geq 2$. Then*

$$\operatorname{ord}_p\left(\tfrac{p-1}{6}!\right) = 2^L \quad \text{or} \quad \operatorname{ord}_p\left(\tfrac{p-1}{6}!\right) = 3 \cdot 2^L, \qquad \ell - 3 \leq L \leq \ell. \tag{4.15}$$

Furthermore, if $\ell = 0$, then $L = 0, 1$ or 2.

Proof. By Theorem 4.10 we have

$$\tfrac{p-1}{3}! \equiv (-1)^{\frac{p-1}{6}+1} u \left(\tfrac{p-1}{6}!\right)^2 \pmod p. \tag{4.16}$$

Raising both sides to the (even) power $3 \cdot 2^{\ell-1}$, we get

$$\left(\tfrac{p-1}{3}!\right)^{3\cdot 2^{\ell-1}} \equiv u^{3\cdot 2^{\ell-1}} \left(\tfrac{p-1}{6}!\right)^{3\cdot 2^{\ell}} \pmod p. \tag{4.17}$$

Now, by Definition 4.1, the left-hand side of (4.17) is $\equiv -1 \pmod p$, and by Lemma 4.9 and Corollary 4.5 we have

$$u^{3\cdot 2^{\ell-1}} \equiv r^{3\cdot 2^{\ell-1}} \equiv (-1)^3 = -1 \pmod p,$$

so that (4.17) reduces to

$$\left(\tfrac{p-1}{6}!\right)^{3\cdot 2^{\ell}} \equiv 1 \pmod p,$$

which gives (4.15) with $L \leq \ell$. To obtain a lower bound for L, we note it was shown in [11, Corollary 2] — which is actually an easy consequence of (3.11) in Proposition 3.12 — that the values of the ratios $\operatorname{ord}_p(\frac{p-1}{6}!)/\operatorname{ord}_p(\frac{p-1}{3}!)$ are restricted to the 18 values

$$\frac{1}{24}, \frac{1}{12}, \frac{1}{8}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{3}{8}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, 1, \frac{4}{3}, \frac{3}{2}, 2, 3, 4, 6, 12,$$

and it is obvious that the largest deviation in the powers of 2 is 3 (in 1/24 and 1/8).

Finally, for $\ell = 0$, we have $r = 1$ by Corollary 4.5; we raise both sides of (4.16) to the third power and note that by Corollary 4.4 we have $(\frac{p-1}{3}!)^3 \equiv 1 \pmod p$, and Lemma 4.9 gives $u^3 \equiv r^3 \equiv 1 \pmod p$. Hence

$$1 \equiv (-1)^{(p+5)/6} \left(\tfrac{p-1}{6}!\right)^6 \pmod p,$$

and upon squaring we have $(\frac{p-1}{6}!)^{12} \equiv 1 \pmod p$, which means that $\operatorname{ord}_p(\frac{p-1}{6}!)$ is a divisor of 12; i.e., it is of the form 2^L or $3 \cdot 2^L$, with $L = 0$, 1 or 2. ∎

Remark 4.12. Proposition 4.11 raises the question as to whether L can take on all four values in relation to ℓ (when $\ell \geq 2$). This is indeed the case (see Tables 7.4 and 7.5):

(1) For $p = 13$ we compute $\operatorname{ord}_p(\frac{p-1}{3}!) = \operatorname{ord}_p(\frac{p-1}{6}!) = 3 \cdot 2^2$, so $\ell = L = 2$ (compare with Proposition 4.7(c)). For $\ell \geq 3$, no other Jacobi prime $p < 10^{14}$ satisfies $\ell = L$.

(2) For 40 of the 45 nonstandard Jacobi primes $p < 10^{14}$ we have $L = \ell - 1$, the smallest one being $p = 97$, and the largest $p = 69\,803\,955\,978\,241$.

(3) The case $L = \ell - 2$ occurs for the the primes 409, 4729, and 824 717 353.

(4) The only prime with $L = \ell - 3$ is 860 301 577.

In the case $\ell = 0$, a slightly more detailed proof of the last part of Proposition 4.11 would show that

$$\begin{aligned} &\operatorname{ord}_p(\tfrac{p-1}{3}!) = 1 \quad \text{implies} \quad \operatorname{ord}_p(\tfrac{p-1}{6}!) = 3, 6, \text{ or } 12; \\ &\operatorname{ord}_p(\tfrac{p-1}{3}!) = 3 \quad \text{implies} \quad \operatorname{ord}_p(\tfrac{p-1}{6}!) = 1, 2, 3, 4, 6, \text{ or } 12. \end{aligned}$$

In both cases, all the orders on the right are actually attained.

5. The main results

5.1. **Preliminaries.** In this section we will state and prove our main theorems concerning solutions of (2.5) and (2.6). In addition to the crucial concept of a Jacobi prime introduced in the previous section, we also need the notion of an *α-exceptional prime* which was introduced and studied in [8], with further properties and criteria in [11]. Recall that in connection with the congruence (4.1) and the subsequent motivation for the definition of a Jacobi prime, we alluded to the sequence of orders $\gamma_1^{(M)}(p)$, $\gamma_2^{(M)}(p), \ldots$ behaving in a very specific way. In fact, Proposition 4.2 in [8] can be simplified as follows, using the notation of (4.2).

Lemma 5.1. *Let $M \geq 2$ and $p \equiv 1 \pmod{M}$ be a prime. Then for a fixed $\alpha \geq 1$,*

$$\frac{\gamma_{\alpha+1}^{(M)}(p)}{\gamma_\alpha^{(M)}(p)} = \frac{p}{2}, p \text{ or } 2p \qquad \text{or} \qquad \frac{\gamma_{\alpha+1}^{(M)}(p)}{\gamma_\alpha^{(M)}(p)} = \frac{1}{2}, 1 \text{ or } 2. \tag{5.1}$$

It turns out that for any given $M \geq 3$, the second alternative in (5.1) is exceedingly rare. This gives rise to the following definition.

Definition 5.2. Given an integer $M \geq 2$, a prime $p \equiv 1 \pmod{M}$ is called α-exceptional for M if the second alternative in (5.1) holds for $\alpha \geq 1$.

Example 5.3. Using computer algebra, it is easy to evaluate

$$\gamma_1^{(4)}(5) = 1, \ \gamma_2^{(4)}(5) = 10; \quad \gamma_1^{(3)}(13) = 12, \ \gamma_2^{(3)}(13) = 12,$$

so $p = 5$ is not 1-exceptional for $M = 4$, while $p = 13$ is 1-exceptional for $M = 3$.

We require the following properties of exceptionality. For proofs, see Theorem 3 and Corollary 3, respectively, in [11].

Lemma 5.4. (a) *Let $M \geq 2$ and $p \equiv 1 \pmod{M}$ be a prime. If p is α-exceptional ($\alpha \geq 2$) for M, then it is also $(\alpha - 1)$-exceptional for M.*

(b) *Let $p \equiv 1 \pmod{6}$ be a prime and $\alpha \geq 1$. Then p is α-exceptional for $M = 3$ if and only if it is α-exceptional for $M = 6$.*

Remark 5.5. (1) Since this paper is almost exclusively concerned with the cases $M = 3$ and $M = 6$, we will call an α-exceptional prime for $M = 3$ (and thus for $M = 6$) simply *α-exceptional*.

(2) Up to 10^{12} only $p = 13$, $p = 181$, $p = 2\,521$, $p = 76\,543$ and $p = 489\,061$ are 1-exceptional. By Lemma 5.4(a), only these primes need to be checked for 2-exceptionality; none of them have this property.

We are now ready to state and prove our main results. If we consider *cubes* of the left-hand sides of (2.5) and (2.6), we can actually establish necessary and sufficient conditions of the solutions; the original congruences will then be discussed later.

5.2. **The case $s \geq 2$.** For simplicity of the statements, we treat the case $s \geq 2$ separately from the cases $s = 0$ and $s = 1$, which will be stated and proved following Theorems 5.6 and 5.8. We begin with the "denominator 3" case.

Theorem 5.6. *Let n be as in (2.4), with $\alpha \geq 1$ and $s \geq 2$. Then a necessary and sufficient condition for*

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{n} \tag{5.2}$$

to hold is that all of the following be satisfied:

(a) *p is $(\alpha-1)$-exceptional if $\alpha > 1$;*
(b) *p is a level-ℓ Jacobi prime for some $0 \leq \ell \leq s$;*
(c) *$q_i^{\beta_i}$ divides $(p-1)(p+1)(p^2+1)\dots(p^{2^{s-2}}+1)$ for all $1 \leq i \leq s$.*

Proof. (i) We first prove the necessity of the conditions (a)–(c). We have already seen at the beginning of Section 4 that (5.2) implies the congruence (4.1). But (4.1) implies that $\gamma_\alpha^{(3)}(p)$ divides $3 \cdot 2^s$. If $\alpha \geq 2$, this means that the first alternative in (5.1) cannot hold (for $\alpha - 1$ in place of α), so p is $(\alpha-1)$-exceptional. If $\alpha = 1$, the condition (a) is vacuous.

Furthermore, we already saw following (4.1) that condition (b) must hold. Finally, the necessity of condition (c) follows from Proposition 3.4 and the Chinese Remainder Theorem.

(ii) For the opposite direction, we first note that condition (b) implies

$$\left(\tfrac{p^\alpha-1}{3}\right)_p !^{3\cdot 2^\ell} \equiv 1 \pmod{p^\alpha}. \tag{5.3}$$

Since $s \geq \ell$, we raise both sides to the power $2^{s-\ell}$, which gives (5.3) with s in place of ℓ. Substituting this into the closed-form congruence (3.8) and cubing, we immediately get

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{p^\alpha}. \tag{5.4}$$

Finally, condition (c) means that the other closed-form congruence, namely (3.3), holds. Cubing it and combining it with (5.4) via the Chinese Remainder Theorem gives (5.2); this completes the proof. ∎

Remark 5.7. Theorem 5.6 shows that for the case $\alpha > 1$ to occur, p has to be 1-exceptional (note Lemma 5.4(a)) and at the same time a Jacobi prime. First, it is readily checked that of the five known exceptional primes up to 10^{12} (see Remark 5.5(2)), $p = 13$ is the only one that is also a Jacobi prime. Second, by Theorem 10 in [11], combined with Proposition 4.7(a), a level-0 Jacobi prime cannot be exceptional. Finally, the ten higher-level Jacobi primes between 10^{12} and 10^{14} are easily checked, using the criterion in Corollary 5 of [11], and found to be nonexceptional.

In summary, $p = 13$ is the only prime $p \equiv 1 \pmod 6$ up to 10^{14} for which n can possibly be a solution of (2.5), where $n = p^\alpha w$ with $\alpha \geq 2$ and w as in (2.4). See also Example 2.3.

We now state the "denominator 6" analogue of Theorem 5.6. The proof is almost identical with that of Theorem 5.6, with the main ingredients again found in Section 3.

Theorem 5.8. *Let the odd integer n be as in* (2.4)*, with $\alpha \geq 1$ and $s \geq 2$. Then a necessary and sufficient condition for*

$$\left\lfloor \tfrac{n-1}{6} \right\rfloor_n !^3 \equiv 1 \pmod{n} \tag{5.5}$$

to hold is that all of the following be satisfied:

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

(b) *p is a Jacobi prime, and $0 \leq L \leq s$;*

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

Remark 5.9. Two subtle but important differences between Theorems 5.6 and 5.8 must be highlighted at this point.

(i) In the conditions (c), note the highest powers 2^{s-2}, resp. 2^{s-1}.

(ii) In Theorem 5.8, $q = 2$ cannot be a factor of n, but $2 \equiv -1 \pmod 3$, and is therefore an allowable factor of n in Theorem 5.6. While an odd prime q can divide at most one of the factors in (c), $q = 2$ divides $p^{2^j}+1$ exactly once for $j \geq 1$. Also, 2 divides one of $p-1$ and $p+1$ exactly once, while it divides the other to a higher power. This is illustrated in Examples 2.2 and 2.3.

5.3. **The cases $s = 0$ and $s = 1$.** We now address the cases that were not covered by Theorems 5.6 and 5.8. We begin with $s = 0$, i.e., the case $w = 1$ in (2.4).

Proposition 5.10. *Let $p \equiv 1 \pmod 3$ be a prime and $\alpha \geq 1$. Then*

$$\left(\tfrac{p^\alpha-1}{3}\right)_p !^3 \equiv 1 \pmod{p^\alpha} \tag{5.6}$$

if and only if $\alpha = 1$ and p is a level-0 Jacobi prime.

Proof. If $\alpha = 1$ and p is a level-0 Jacobi prime, then (5.6) holds by Definition 4.1. Now assume that (5.6) holds, and note that it implies $\gamma_\alpha^{(3)}(p) = 1$ or 3. We now appeal to a more detailed version of Lemma 5.1, given as Proposition 4.2 in [8], which says that in this particular case the right-hand alternative in (5.1) is always 1 (mod p), and since $p \neq 3$, this forces $\gamma_\alpha^{(3)}(p) = \gamma_{\alpha-1}^{(3)}(p) = \dots = \gamma_1^{(3)}(p)$ when $\alpha > 1$. This means that, first, p is a level-0 Jacobi prime by Definition 4.1 and, second, p is 1-exceptional when $\alpha > 1$. But by Theorem 10 in [11] this is a contradiction to p being of the form $p = 27X^2 + 27X + 7$, i.e., to being a level-0 Jacobi prime. So $\alpha > 1$ is impossible, which completes the proof. ∎

Remark 5.11. (1) If p satisfies (5.6) with $\alpha = 1$, i.e.,

$$\left(\tfrac{p-1}{3}!\right)^3 \equiv 1 \pmod{p}, \tag{5.7}$$

then $\operatorname{ord}_p(\frac{p-1}{3}!) = 1$ or 3 (or equivalently $r = 1$); see the $\gamma_1^3(p)$ column in Table 7.1. Can one distinguish between these two cases? We have not been able to find a criterion, and we believe this to be a difficult question.

(2) However, we can make the following observations. By (5.7), $\frac{p-1}{3}!$ is a cube root of unity (mod p). On the other hand, by Lemma 4.9 and Corollary 4.5 we have $u^3 \equiv r^3 \equiv 1 \pmod p$, so u is also a cube root of unity (mod p), and so is u^2. Since, by Proposition 4.7, $p = 27X^2 + 27X + 7$, it is easily derived from the parametric representations at the end of Section 4.1 that $u = -9X - 5$ for even X, while $u = 9X + 4$ for odd X, and, in particular, $u \neq 1$ for a standard Jacobi

prime p. Thus 1, u, and u^2 are the three distinct cube roots of unity (mod p), and one might expect that the three cases

$$\tfrac{p-1}{3}! \equiv 1 \pmod p, \qquad \tfrac{p-1}{3}! \equiv u \pmod p, \qquad \tfrac{p-1}{3}! \equiv u^2 \pmod p \tag{5.8}$$

occur, on average, equally often. Indeed, computations show that of the 3121 primes $p = 27X^2 + 27X + 7 < 10^{10}$, the three congruences in (5.8) are satisfied by 1037, 1030, and 1054 of them, respectively.

Proposition 5.12. *Let $p \equiv 1 \pmod 6$ be a prime and $\alpha \geq 1$. Then a necessary condition for*

$$\left(\tfrac{p^\alpha-1}{6}\right)_p ! \equiv 1 \pmod{p^\alpha} \tag{5.9}$$

to hold is that either

(i) *p is a standard Jacobi prime, in which case $\alpha = 1$, or*

(ii) *p is a level-3 Jacobi prime which is $\alpha - 1$ exceptional when $\alpha > 1$.*

Proof. The congruence (5.9) means, in particular, that $\gamma_\alpha^{(6)}(p) = 1$. Once again Lemma 5.1 implies that p must be a 1-exceptional prime if $\alpha > 1$. In this case a refinement of Lemma 5.1 (Proposition 4.2 in [8]) means that the sequence of orders $(\gamma_1^{(6)}(p), \gamma_2^{(6)}(p), \dots, \gamma_\alpha^{(6)}(p))$ can only occur as $(1, 1, \dots, 1, 1)$, $(1, 2, 1, \dots, 2, 1)$, or $(2, 1, 2, \dots, 2, 1)$. In particular, this implies that $\gamma_1^{(6)}(p) = 1$ or 2, i.e., $(\frac{p-1}{6}!)^2 \equiv 1 \pmod p$ in all cases.

Now we proceed with a similar argument as in the proof of Proposition 4.11 and note that (4.16) implies

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

Raising this to the sixth power and using Corollary 4.4 on the left and Lemma 4.9 on the right, we get $1/r^2 \equiv r^6 \pmod p$, i.e., $r^8 \equiv 1 \pmod p$. This means, by Corollary 4.5, that p is a Jacobi prime of level $0 \leq \ell \leq 3$.

When $\ell = 0$, then p cannot be 1-exceptional, as we have already seen. This implies $\alpha = 1$, which is part (i) of our result. Next, $\ell = 1$ is impossible by Proposition 4.7(b), while by Proposition 4.7(c), $p = 13$ is the only candidate for $\ell = 2$. However, it is easy to see that $\gamma_1^{(6)}(13) = 12$, and therefore there cannot be a solution of (5.9) with $p = 13$. This leaves $\ell = 3$, which is part (ii) of this result. ∎

Remark 5.13. (1) The first few solutions of (5.9) in case (i) are $p = 7$, 74 419 (see Table 7.1), 1 409 731, 1 600 891, ..., with a total of 253 up to 10^{10}. Again we have $p = 27X^2 + 27X + 7$, i.e., $(\frac{p-1}{3}!)^3 \equiv 1 \pmod p$, and upon cubing both sides of the congruence (4.16), we see that $(\frac{p-1}{6}!)^6 \equiv 1 \pmod p$ if and only if $p \equiv 7 \pmod{12}$. Thus $(\frac{p-1}{6}!)^2$ is a cube root of unity (mod p), and we might expect that the cases

$$\left(\tfrac{p-1}{3}!\right)^2 \equiv 1 \pmod p, \quad \left(\tfrac{p-1}{3}!\right)^2 \equiv u \pmod p, \quad \left(\tfrac{p-1}{3}!\right)^2 \equiv u^2 \pmod p \tag{5.10}$$

occur, on average, equally often. Indeed, computations show that of the 1555 primes $p = 27X^2 + 27X + 7 < 10^{10}$ that are 7 (mod 12), the congruences in (5.10) are satisfied by 499, 542, and 514 of them, respectively. Of the 499 that satisfy the first congruence in (5.10), 253 (resp. 246) satisfy $\frac{p-1}{6}! \equiv 1 \pmod p$ (resp. $\equiv -1 \pmod p$). It is reasonable to expect one-twelfth of all primes $p = 27X^2 + 27X + 7$ to satisfy $\frac{p-1}{6}! \equiv 1 \pmod p$.

(2) The only level-3 Jacobi primes up to 10^{14} (see Tables 7.4 and 7.5) are $p = 409$, 4 729, 824 717 353, and 860 301 577. Only the last one of these has $L = 0$ (see Table 7.5). However, $\gamma_1^{(6)}(p) = 3 \cdot 2^0$, so this prime, while being a solution of the cube of (5.9), is not a solution of (5.9) itself.

We now turn to the case $s = 1$ and begin with the analogue of Theorem 5.6.

Proposition 5.14. (a) *Let $n = p^\alpha q^\beta$, with primes $p \equiv 1 \pmod 3$ and $q \equiv -1 \pmod 3$, and integers $\alpha, \beta \geq 1$, except when $q = 2$, in which case $\beta \geq 2$. Then a necessary and sufficient condition for* (5.2) *to hold is that $\alpha = 1$, p is a standard Jacobi prime, and $q^\beta \mid p - 1$.*

(b) *If $n = 2p^\alpha$, with p and α as in part (a), then the only solutions of* (2.5) *are $2 \cdot 13$ and $2 \cdot 13^2$.*

Proof. (a) The proof is identical with that of Theorem 5.6, with the product of $p - 1$ and the generalized Fermat numbers replaced by only $p - 1$, according to Proposition 3.4. Condition (b) means that, in fact, $\ell = 0$ since by Proposition 4.7(b) there are no level-1 Jacobi primes. Finally, as we saw before, such a p cannot be $(\alpha - 1)$-exceptional for any $\alpha \geq 2$, which forces $\alpha = 1$.

(b) In this case we have $\varepsilon(n) = -1$ in Lemma 3.10, and upon cubing both sides of (3.8) we find that $n = 2p^\alpha$ is a solution of (5.2) if

$$(\tfrac{p^\alpha - 1}{3})_p!^6 \equiv -1 \pmod{p^\alpha}.$$

But this means that $\gamma_\alpha^{(3)}(p) = 1, 2, 3, 4, 6$, or 12. By the refinement of Lemma 5.1 already mentioned in the proof of Proposition 5.10, this means that p is a Jacobi prime of level 0, 1 or 2 and is $(\alpha - 1)$-exceptional when $\alpha > 1$. By Proposition 4.7, level 1 is impossible, while the only level-2 Jacobi prime is $p = 13$, which is also 1-exceptional, but not 2-exceptional. Hence the only possible solutions with a nonstandard Jacobi prime are $n = 2 \cdot 13$ and $n = 2 \cdot 13^2$. Table 2.1 shows that these two numbers are in fact solutions of (2.5).

This leaves the case where p is a standard Jacobi prime, which also means that $\alpha = 1$, as we have seen earlier. If $n = 2p$ were a solution of (2.5), then by (3.8) we would have

$$2^{(p-1)/3}(\tfrac{p-1}{3}!)^2 \equiv -1 \pmod p.$$

Multiplying both sides by $\frac{p-1}{3}!$ and using the fact that p is a level-0 Jacobi prime, we get

$$2^{(p-1)/3} \equiv -\tfrac{p-1}{3}! \pmod p.$$

Finally, cubing both sides of this congruence and once again using $(\frac{p-1}{3}!)^3 \equiv 1 \pmod p$, we obtain $1 \equiv -1 \pmod p$, which is a contradiction. This means that there are no solutions with p a standard Jacobi prime, which completes the proof. ∎

Example 5.15. (a) Let $p = 61$. Then $p - 1 = 2^2 \cdot 3 \cdot 5$, and $61 \cdot 2^2$ and $61 \cdot 5$ are solutions of (5.2). By computation we find that both are also solutions of the original congruence (2.5); see Table 2.1.

(b) With $p = 1951$ we obtain $p - 1 = 2 \cdot 3 \cdot 5^2 \cdot 13$, so Proposition 5.14 gives $n = 1951 \cdot 5$ and $n = 1951 \cdot 5^2$ as solutions of (5.2). Once again, as Table 2.1 shows, both are solutions of (2.5).

Finally in this section, we deal with the case $s = 1$ and denominator 6.

Proposition 5.16. *Let $n = p^\alpha q^\beta$, with primes $p \equiv 1 \pmod 6$, $q \equiv -1 \pmod 6$ and integers $\alpha, \beta \geq 1$. Then a necessary condition for* (2.6) *to hold is that either*

(i) *p is a standard Jacobi prime and $q^\beta \mid p^2 - (\frac{p}{q})(-1)^{(p-1)/2}$, in which case $\alpha = 1$, or*

(ii) *p is a level-3 Jacobi prime which is $(\alpha-1)$-exceptional when $\alpha > 1$, and $q^\beta \mid p^2 - (\frac{p}{q})$.*

Proof. As usual, we apply the Chinese Remainder Theorem, in this case combining the congruences (3.6) and (3.9). We begin by considering the latter. Assuming that n is a solution of (2.6), we raise both sides of (3.9) to the sixth power, obtaining the congruence (5.9). Proposition 5.12 then gives necessary conditions for its solution.

The second condition in each of the cases (i) and (ii) follows directly from Proposition 3.7. Now, it is a consequence of Corollary 4.5 that a Jacobi prime p of level $\ell \geq 2$ always satisfies $p \equiv 1 \pmod 4$. This implies that $(-1)^{(p-1)/2} = 1$, which gives the second condition in (ii). □

Example 5.17. (a) Let $p = 1951$, a standard Jacobi prime. We have $1951^2 + 1 = 2{\cdot}17{\cdot}111953$. Both $q = 17$ and 111953 satisfy $q \equiv -1 \pmod 6$ and $(\frac{p}{q})(-1)^{(p-1)/2} = -1$. While $n = 1951 \cdot 111953$ is a solution of (2.6), $n = 1951 \cdot 17$ is not (it would be a solution of the cube of the congruence).

Next, $1951^2 - 1 = 2^6 \cdot 3 \cdot 5^2 \cdot 13 \cdot 61$. Here only $q = 5$ satisfies $q \equiv -1 \pmod 6$, but $(\frac{p}{q})(-1)^{(p-1)/2} = -1$, so $n = 1951 \cdot 5^\beta$ cannot be a solution for any $\beta \geq 1$.

(b) As in Remark 5.13, we note that there are only four level-3 Jacobi primes up to 10^{14}. Combining Proposition 5.16(ii) with computations, we find that these primes lead to one single solution, namely $n = 824\,717\,353 \cdot 5$.

6. Proofs of the closed-form congruences

In this section we will prove the crucial closed-form congruences that were stated in Section 3, namely Lemmas 3.1, 3.2, 3.10 and 3.11. We will actually prove more general results which then immediately imply the lemmas in question, as well as Lemmas 2–4 in [10] which correspond to the case $M = 4$. The proofs are modeled after those in [10].

6.1. Congruences modulo w.

Proposition 6.1. *Let $M \geq 3$ and $s \geq 1$ be integers, and let $n = p^\alpha w$, $w = q_1^{\beta_1} \dots q_s^{\beta_s}$, where $p, q_1, \dots, q_s$ are distinct primes with $p \equiv 1 \pmod M$ and $q_1 \equiv \dots \equiv q_s \equiv -1 \pmod M$. Then*

$$\lfloor \tfrac{n-1}{M} \rfloor_n ! \equiv \frac{B_s(n)}{p^{\varphi(M,1,w)}} \pmod w, \tag{6.1}$$

where $\varphi(M,1,w)$ is as defined in (3.1)*, and*

$$B_s(n) = \begin{cases} (-1)^{(p-1)/M}, & s = 1, \\ 1, & s \geq 2. \end{cases}$$

Proof. With $m := \frac{p^\alpha - 1}{M}$, we have for $n \equiv 1 \pmod M$, resp. $n \equiv -1 \pmod M$,

$$\tfrac{n-1}{M} = mw + \tfrac{w-1}{M}, \quad \text{resp.} \quad \tfrac{n-M+1}{M} = mw + \tfrac{w-M+1}{M},$$

and thus in either case, $\left\lfloor \frac{n-1}{M} \right\rfloor = mw + \left\lfloor \frac{w}{M} \right\rfloor$. Based on this, we write

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! = \Big(\prod_{j=1}^{m} P_j\Big) Q, \tag{6.2}$$

where we have, for all $j = 1, \dots, m$,

$$P_j := \prod_{\substack{k=1 \\ \gcd((j-1)w+k,n)=1}}^{w} \big((j-1)w+k\big), \qquad Q := \prod_{\substack{k=1 \\ \gcd(mw+k,n)=1}}^{\lfloor w/M \rfloor} \big(mw+k\big).$$

We now define the corresponding 'augmented' products

$$\overline{P_j} := \prod_{\substack{k=1 \\ \gcd((j-1)w+k,w)=1}}^{w} \big((j-1)w+k\big), \qquad \overline{Q} := \prod_{\substack{k=1 \\ \gcd(mw+k,w)=1}}^{\lfloor w/M \rfloor} \big(mw+k\big),$$

so the products $\overline{P_j}$ and $\overline{Q}$ include multiples of p that are relatively prime to w. Now for $1 \le j \le m$, the Gauss-Wilson Theorem gives

$$\begin{aligned} \overline{P_j} &\equiv \prod_{\substack{k=1 \\ \gcd(k,w)=1}}^{w} k \\ &= (w-1)_w ! \equiv \begin{cases} -1 \pmod w & \text{if } s = 1 \text{ for all } M, \\ -1 \pmod w & \text{if } s = 2, M = 3, q_1 = 2, \beta_1 = 1, \\ 1 \pmod w & \text{if } s \ge 2 \text{ in all other cases,} \end{cases} \end{aligned} \tag{6.3}$$

and we also have

$$\overline{Q} \equiv \prod_{\substack{k=1 \\ \gcd(k,w)=1}}^{\lfloor w/M \rfloor} k = \left\lfloor \tfrac{w-1}{M} \right\rfloor_w ! \pmod w. \tag{6.4}$$

The product $\overline{P_1} \cdots \overline{P_m} \cdot \overline{Q}$ can be reduced to (6.2) by dividing the former by

$$\Pi_1 := \prod_{\substack{\nu=1 \\ \gcd(\nu,w)=1}}^{m_1} (\nu p), \tag{6.5}$$

where

$$m_1 = \begin{cases} \dfrac{p^{\alpha-1}w-1}{M} = \dfrac{p^{\alpha-1}-1}{M} w + \dfrac{w-1}{M}, & n \equiv 1 \pmod M, \\ \dfrac{p^{\alpha+1-M}w-1}{M} = \dfrac{p^{\alpha-1}-1}{M} w + \dfrac{w+1-M}{M}, & n \equiv -1 \pmod M, \end{cases}$$

and in either case,

$$m_1 = M_1 w + \left\lfloor \tfrac{w-1}{M} \right\rfloor, \qquad M_1 := \frac{p^{\alpha-1}-1}{M}. \tag{6.6}$$

With (6.5) and (6.6) we then have

$$\begin{aligned} \Pi_1 &\equiv \Big(p^{\varphi(w)}(w-1)_w !\Big)^{M_1} p^{\varphi(M,1,w)} \left\lfloor \tfrac{w-1}{M} \right\rfloor_w ! \pmod w \\ &\equiv (-1)^{b(s)M_1} p^{\varphi(M,1,w)} \left\lfloor \tfrac{w-1}{M} \right\rfloor_w ! \pmod w, \end{aligned} \tag{6.7}$$

where $b(s) = 1$ when $s = 1$ or $s = 2$, $M = 3$, $q_1 = 2$ and $\beta_1 = 1$, and $b(s) = 0$ when $s \geq 2$, having used the theorems of Euler-Fermat and Gauss-Wilson. Now with (6.2)–(6.4) and (6.7),

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv \frac{\overline{P_1} \cdots \overline{P_m} \cdot \overline{Q}}{\Pi_1} \equiv \frac{(-1)^{b(s)(m-M_1)}}{p^{\varphi(M,1,w)}} \pmod{w}. \tag{6.8}$$

Finally, we note that

$$m - M_1 = \frac{p^\alpha - 1}{M} - \frac{p^{\alpha-1} - 1}{M} = \frac{p^{\alpha-1}(p-1)}{M} \equiv \frac{p-1}{M} \pmod 2,$$

and this, with (6.8), gives (6.1). □

We note that Proposition 6.1 is also valid for $M = 2$; this is the case treated in [7]. However, it is essential for the current paper to have $1 \not\equiv -1 \pmod M$.

Proof of Lemmas 3.1 *and* 3.2. The first parts of (3.2), (3.3) are immediate consequences of (6.1), where in the case $M = 3$ we note that $(p-1)/3$ is always even, so that $B_s(n) = 1$ also for $s = 1$. The evaluations of $\varphi(M, 1, w)$ follow directly from [23], Theorem 5 (for $M = 3$) and Theorem 7 (for $M = 6$). □

6.2. **Congruences modulo p^α.** In this larger subsection we prove congruences that will give Lemmas 3.10 and 3.11, as well as Lemmas 2 and 3 in [10], as special cases.

Proposition 6.2. *Let $M \geq 3$ and $s \geq 1$ be integers, and let $n = p^\alpha w$, $w = q_1^{\beta_1} \dots q_s^{\beta_s}$, where $p, q_1, \dots, q_s$ are distinct primes with $p \equiv 1 \pmod M$ and $q_1 \equiv \dots \equiv q_s \equiv -1 \pmod M$. If $n \equiv \delta \pmod M$, with $\delta \in \{-1, 1\}$, then for $s = 1$,*

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv (-1)^E q_1^{\delta\varphi(p^\alpha)/M} \left(\frac{p^\alpha - 1}{M} \right)_p !^{2\delta} \pmod{p^\alpha}, \tag{6.9}$$

where

$$E = \begin{cases} 0, & \text{when } M = 3, q_1 = 2, \beta_1 \geq 2, \\ (p + q_1)/M, & \text{otherwise,} \end{cases}$$

while for $s \geq 2$,

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv (q_1 \dots q_s)^{\delta 2^{s-1}\varphi(p^\alpha)/M} \left(\frac{p^\alpha - 1}{M} \right)_p !^{\delta 2^s} \pmod{p^\alpha}. \tag{6.10}$$

Proof. 1. By considering the two cases $\delta = \pm 1$ separately, it is easy to verify that

$$\left\lfloor \frac{n-1}{M} \right\rfloor = \left\lfloor \frac{w-1}{M} \right\rfloor p^\alpha + \gamma \frac{p^\alpha - 1}{M}, \qquad \gamma = \begin{cases} 1 & \text{if } \delta = 1, \\ M - 1 & \text{if } \delta = -1. \end{cases}$$

Based on this, we write

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! = \left(\prod_{j=1}^{\lfloor \frac{w-1}{M} \rfloor} P_j \right) Q, \tag{6.11}$$

where

$$P_j := \prod_{\substack{k=1 \\ \gcd((j-1)p^\alpha + k, n) = 1}}^{p^\alpha - 1} \big((j-1)p^\alpha + k \big), \quad Q := \prod_{\substack{k=1 \\ \gcd(\lfloor \frac{w-1}{M} \rfloor p^\alpha + k, n) = 1}}^{\gamma \frac{p^\alpha - 1}{M}} \left(\left\lfloor \tfrac{w-1}{M} \right\rfloor p^\alpha + k \right).$$

With the goal of evaluating these modulo p^α, we define the related easier products

$$\overline{P_j} := \prod_{\substack{k=1 \\ \gcd((j-1)p^\alpha+k,p)=1}}^{p^\alpha-1} \big((j-1)p^\alpha+k\big), \quad \overline{Q} := \prod_{\substack{k=1 \\ \gcd(\lfloor \frac{w-1}{M} \rfloor p^\alpha+k,p)=1}}^{\gamma\frac{p^\alpha-1}{M}} \left(\left\lfloor \tfrac{w-1}{M} \right\rfloor p^\alpha+k\right),$$

which include multiples of the primes q_i that are relatively prime only to p. We do this because the $\overline{P_j}$ and $\overline{Q}$ are easy to evaluate modulo p^α. In fact, we have

$$\overline{P_j} \equiv \prod_{\substack{k=1 \\ \gcd(k,p)=1}}^{p^\alpha-1} k = (p^\alpha-1)_p! \equiv -1 \pmod{p^\alpha} \tag{6.12}$$

by the Gauss-Wilson theorem (2.1), and

$$\overline{Q} \equiv \prod_{\substack{k=1 \\ \gcd(k,p)=1}}^{\gamma\frac{p^\alpha-1}{M}} k = \left(\gamma\tfrac{p^\alpha-1}{M}\right)_p! \pmod{p^\alpha}. \tag{6.13}$$

To evaluate the right-hand side of (6.13) in the case $\delta = -1$, we note that by the Gauss-Wilson theorem we have

$$\left((M-1)\tfrac{p^\alpha-1}{M}\right)_p! \prod_{\substack{k=1 \\ \gcd(k,p)=1}}^{\frac{p^\alpha-1}{M}} (p^\alpha-k) = (p^\alpha-1)_p! \equiv -1 \pmod{p^\alpha}. \tag{6.14}$$

But we have

$$\prod_{\substack{k=1 \\ \gcd(k,p)=1}}^{\frac{p^\alpha-1}{M}} (p^\alpha-k) \equiv (-1)^A \left(\tfrac{p^\alpha-1}{M}\right)_p! \pmod{p^\alpha}, \tag{6.15}$$

where A is the number of terms in the product on the left, which we can count as follows. For $\alpha = 1$, we clearly have $A = (p-1)/M$. When $\alpha \geq 2$, we divide by p with remainder:

$$\frac{p^\alpha-1}{M} = \frac{p-1}{M}\left(p^{\alpha-2}+\cdots+1\right)p + \frac{p-1}{M}.$$

This means that the number of terms in the ordinary factorial product $((p^\alpha-1)/M)!$ that are divisible by p is $(p-1)(p^{\alpha-2}+\cdots+1)/M$, and using a factorization of the total number $(p^\alpha-1)/M$, we find that the number of terms in the Gauss factorial product $((p^\alpha-1)/M)_p!$ in (6.15) is

$$\begin{aligned} A &= \frac{p-1}{M}\left(p^{\alpha-1}+p^{\alpha-2}+\cdots+1\right) - \frac{p-1}{M}\left(p^{\alpha-2}+\cdots+1\right) \\ &= \frac{p-1}{M}p^{\alpha-1} \equiv \frac{p-1}{M} \pmod 2. \end{aligned}$$

So we have $A \equiv (p-1)/M \pmod 2$ for all $\alpha \geq 1$, and (6.13)–(6.15) now give

$$\overline{Q} \equiv \left((-1)^{\frac{p-1}{M}-1}\right)^{\frac{\delta-1}{2}} \left(\tfrac{p^\alpha-1}{M}\right)_p!^\delta \pmod{p^\alpha}. \tag{6.16}$$

2. The product of $\overline{Q}$ and the $\overline{P_j}$, $j = 1, \ldots, \lfloor \frac{w-1}{M} \rfloor$, is the product of all integers from 1 to $\lfloor \frac{n-1}{M} \rfloor$, without multiples of p. To reduce this $\lfloor \frac{n-1}{M} \rfloor_n!$ in (6.11), we use the inclusion/exclusion principle and first divide the product by all the multiples of

$q_1, \dots, q_s$, then multiply it by all the multiples (if any) of $q_{j_1}q_{j_2}$, $1 \le j_1 < j_2 \le s$, then divide by all the multiples (if any) of $q_{j_1}q_{j_2}q_{j_3}$, $1 \le j_1 < j_2 < j_3 \le s$, etc. To do this, we define for a given k, $1 \le k \le s$ and $1 \le j_1 < \cdots < j_k \le s$, the product

$$\Pi(j_1, \dots, j_k) = \prod_{\substack{\nu=1 \\ \gcd(\nu,p)=1}}^{m(j_1,\dots,j_k)} (\nu q_{j_1} \dots q_{j_k}), \quad m(j_1, \dots, j_k) := \left\lfloor \frac{\lfloor (n-1)/M \rfloor}{q_{j_1} \dots q_{j_k}} \right\rfloor. \tag{6.17}$$

It is straightforward to verify that

$$m(j_1, \dots, j_k) = \begin{cases} \frac{1}{M}(w(\mathbf{j}) - 1)p^\alpha + \frac{p^\alpha - 1}{M}, & (-1)^k = \delta, \\ \frac{1}{M}(w(\mathbf{j}) - M + 1)p^\alpha + (M-1)\frac{p^\alpha - 1}{M}, & (-1)^k = -\delta, \end{cases} \tag{6.18}$$

where $w(\mathbf{j}) := w/(q_{j_1} \dots q_{j_k})$. With the notation

$$M(j_1, \dots, j_k) := \begin{cases} \frac{1}{M}(w(\mathbf{j}) - 1), & (-1)^k = \delta, \\ \frac{1}{M}(w(\mathbf{j}) - M + 1), & (-1)^k = -\delta, \end{cases} \tag{6.19}$$

we get from (6.17) and (6.18), when $(-1)^k = \delta$,

$$\begin{aligned} \Pi(j_1, \dots, j_k) &\equiv \left[(q_{j_1} \dots q_{j_k})^{\varphi(p^\alpha)} (p^\alpha - 1)_p! \right]^{M(j_1,\dots,j_k)} \\ &\quad \times (q_{j_1} \dots q_{j_k})^{\varphi(p^\alpha)/M} \left(\tfrac{p^\alpha - 1}{M} \right)_p ! \pmod{p^\alpha} \\ &\equiv (-1)^{M(j_1,\dots,j_k)} (q_{j_1} \dots q_{j_k})^{\varphi(p^\alpha)/M} \left(\tfrac{p^\alpha - 1}{M} \right)_p ! \pmod{p^\alpha}, \end{aligned} \tag{6.20}$$

where we have used the Euler-Fermat and the Gauss-Wilson theorems. Similarly, when $(-1)^k = -\delta$,

$$\begin{aligned} \Pi(j_1, \dots, j_k) &\equiv (-1)^{M(j_1,\dots,j_k)} (q_{j_1} \dots q_{j_k})^{(M-1)\varphi(p^\alpha)/M} \\ &\quad \times \left(\tfrac{(M-1)(p^\alpha - 1)}{M} \right)_p ! \pmod{p^\alpha}. \end{aligned} \tag{6.21}$$

Now, for any integer x with $p \nmid x$ the Euler-Fermat theorem gives

$$x^{(M-1)\varphi(p^\alpha)/M} \equiv x^{-\varphi(p^\alpha)/M} \pmod{p^\alpha}. \tag{6.22}$$

This, together with the case $\delta = -1$ of (6.16), applied to (6.21) leads to

$$\begin{aligned} \Pi(j_1, \dots, j_k) &\equiv (-1)^{M(j_1,\dots,j_k) + \frac{p-1}{M} - 1} (q_{j_1} \dots q_{j_k})^{-\varphi(p^\alpha)/M} \\ &\quad \times \left(\tfrac{(p^\alpha - 1)}{M} \right)_p !^{-1} \pmod{p^\alpha} \end{aligned}$$

for $(-1)^k = -\delta$. Raising both sides of this last congruence to the power $(-1)^k = -\delta$, and both sides of (6.20) to the power $(-1)^k = \delta$, we get the following congruence which holds in all cases:

$$\begin{aligned} \Pi(j_1, \dots, j_k)^{(-1)^k} &\equiv (-1)^{M(j_1,\dots,j_k) + \theta} (q_{j_1} \dots q_{j_k})^{\delta\varphi(p^\alpha)/M} \\ &\quad \times \left(\tfrac{p^\alpha - 1}{M} \right)_p !^\delta \pmod{p^\alpha}, \end{aligned} \tag{6.23}$$

where

$$\theta = \begin{cases} 0 & \text{when } \delta = (-1)^k, \\ \frac{p-1}{M} - 1 & \text{when } \delta = -(-1)^k. \end{cases}$$

To conclude this part of the proof, we compare (6.11) with the product of $\overline{Q}$ and $\overline{P_j}$, $j = 1, \dots, \lfloor \frac{w-1}{M} \rfloor$, keeping in mind the remarks made before (6.17). Then

$$\begin{aligned} \left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! &= \left(\prod_{j=1}^{\lfloor \frac{w-1}{M} \rfloor} \overline{P_j} \right) \overline{Q} \prod_{k=1}^{s} \prod_{(\mathbf{j})} \Pi(j_1, \dots, j_k)^{(-1)^k} \\ &\equiv (-1)^{\lfloor \frac{w-1}{M} \rfloor + (\frac{p-1}{M} - 1)\frac{\delta-1}{2}} \left(\tfrac{p^\alpha - 1}{M} \right)_p !^\delta \\ &\quad \times \prod_{k=1}^{s} \prod_{(\mathbf{j})} \Pi(j_1, \dots, j_k)^{(-1)^k} \pmod{p^\alpha}, \end{aligned} \tag{6.24}$$

where $(\mathbf{j})$ indicates that the product is taken over all $1 \le j_1 < \cdots < j_k \le s$. Here we have used (6.12) and (6.16).

3. To complete the proof, we first consider the case $s = 1$. In this case we have $k = 1$, $w = q_1^{\beta_1}$, and $w(\mathbf{j}) = q_1^{\beta_1 - 1}$. From (6.24) and (6.23) we then get

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv (-1)^E q_1^{\delta \varphi(p^\alpha)/M} \left(\tfrac{p^\alpha - 1}{M} \right)_p !^{2\delta} \pmod{p^\alpha}, \tag{6.25}$$

where

$$E = \left\lfloor \tfrac{w-1}{M} \right\rfloor + M(j_1) + \theta + (\tfrac{p-1}{M} - 1)\tfrac{\delta-1}{2} = \left\lfloor \tfrac{w-1}{M} \right\rfloor + M(j_1) + \tfrac{p-1}{M} - 1$$

for both $\delta = 1$ and $\delta = -1$. With (6.19) we then have for $\delta = 1$ and -1, respectively,

$$\begin{aligned} E &= \frac{q_1^{\beta_1} - 1}{M} + \frac{q_1^{\beta_1 - 1} - M + 1}{M} + \frac{p-1}{M} - 1, \\ E &= \frac{q_1^{\beta_1} - M + 1}{M} + \frac{q_1^{\beta_1 - 1} - 1}{M} + \frac{p-1}{M} - 1, \end{aligned}$$

and thus in both cases

$$E = q_1^{\beta_1 - 1} \frac{q_1 + 1}{M} + \frac{p-1}{M} \equiv \frac{q_1 + p}{M} \pmod 2,$$

where the congruence holds whenever q_1 is odd, or $q_1 = 2$ and $\beta_1 = 1$. We can have $q_1 = 2$ only when $M = 3$, in which case $p \equiv 1 \pmod 6$, and thus $E \equiv 0 \pmod 2$ when $\beta \ge 2$. This, together with (6.25), proves (6.9).

4. Now we let $s \ge 2$, and we begin by counting the number of terms $\Pi(j_1, \dots, j_k)$ in the double product in (6.24), separately for even and for odd k:

$$\sum_{k=1}^{s} \sum_{\substack{1 \le j_1 < \cdots < j_k \le s \\ k \text{ even}}} 1 = \sum_{j=1}^{\lfloor \frac{s}{2} \rfloor} \binom{s}{2j} = 2^{s-1} - 1, \tag{6.26}$$

$$\sum_{k=1}^{s} \sum_{\substack{1 \le j_1 < \cdots < j_k \le s \\ k \text{ odd}}} 1 = \sum_{j=0}^{\lfloor \frac{s-1}{2} \rfloor} \binom{s}{2j+1} = 2^{s-1}. \tag{6.27}$$

The evaluations of the binomial sums above are well known and can be found, e.g., in [18], identities (1.97) and (1.89).

To evaluate the right-hand side of (6.24), we first deal with the powers of -1, starting with the exponent θ in (6.23). When $\delta = 1$, resp. -1, then only for odd (resp. even) k is there a contribution $\frac{p-1}{M} - 1$ in each of the factors $\Pi(j_1, \dots, j_k)$, of which there are an even (resp. odd) number, by (6.27), resp. (6.26), and keeping in mind that $s \ge 2$. But this, combined with $(\frac{p-1}{M} - 1)\frac{\delta-1}{2}$ in (6.24), means that the sum of all the θ, plus this last term, is always even and therefore gives no contribution to the sign.

The remaining exponents of -1 add to

$$B := \sum_{k=1}^{s} \sum_{(\mathbf{j})} M(j_1, \dots, j_k) + \left\lfloor \tfrac{w-1}{M} \right\rfloor$$

by (6.24) and (6.23). First let $\delta = 1$. Then by (6.19) we have

$$\begin{aligned} B &:= \sum_{\substack{k=1 \\ k \text{ even}}}^{s} \sum_{(\mathbf{j})} \frac{w(\mathbf{j}) - 1}{M} + \sum_{\substack{k=1 \\ k \text{ odd}}}^{s} \sum_{(\mathbf{j})} \frac{w(\mathbf{j}) - M + 1}{M} + \frac{w-1}{M} \\ &= \frac{w}{M} \sum_{k=1}^{s} \sum_{(\mathbf{j})} \frac{1}{q_{j_1} \dots q_{j_k}} - \frac{1}{M}\left(2^{s-1} - 1\right) - \frac{M-1}{M} 2^{s-1} + \frac{w-1}{M} \\ &= \frac{w}{M} \sum_{k=1}^{s} \sum_{(\mathbf{j})} \frac{1}{q_{j_1} \dots q_{j_k}} - 2^{s-1}, \end{aligned}$$

where in the middle row we have used (6.26) and (6.27). The double sum in the last row can be written as a product; hence we get, along with the definition of w,

$$\begin{aligned} B &= \frac{q_1^{\beta_1} \dots q_s^{\beta_s}}{M} \prod_{j=1}^{s} \left(1 + \frac{1}{q_j}\right) - 2^{s-1} = \frac{1}{M} \prod_{j=1}^{s} q_j^{\beta_j - 1} (q_j + 1) - 2^{s-1} \\ &= q_1^{\beta_1 - 1} \frac{q_1 + 1}{M} \prod_{j=2}^{s} q_j^{\beta_j - 1} (q_j + 1) - 2^{s-1}. \end{aligned}$$

Since $(q_1 + 1)/M$ is always an integer (including the case $M = 3$ and $q_1 = 2$) and $q_j + 1$ is even for $2 \le j \le s$, we see that B is even since $s \ge 2$. The case $\delta = -1$ is completely analogous and also gives an even B. This means that in all cases all the powers of -1 cancel out.

Next, since by (6.26) and (6.27) the double product in (6.24) has $2^s - 1$ terms, the Gauss factorial $(\frac{p^\alpha - 1}{M})_p!^\delta$ occurs to the power 2^s in the desired congruence (6.10).

Finally, it remains to determine the product

$$\prod_{k=1}^{s} \prod_{1 \le j_1 < \dots < j_k \le s} q_{j_1} \dots q_{j_k}. \tag{6.28}$$

We fix an index j, $1 \le j \le s$, and observe that for a given k, $1 \le k \le s$, the number of times the prime q_j occurs in the products $q_{j_1} \dots q_{j_k}$ is $\binom{s-1}{k-1}$ (since j is fixed and the remaining $k - 1$ subscripts vary). So q_j occurs a total of

$$\sum_{k=1}^{s} \binom{s-1}{k-1} = \sum_{k=0}^{s-1} \binom{s-1}{k} = 2^{s-1}$$

times in (6.28). Since this is independent of j, we have

$$\prod_{k=1}^{s}\prod_{(\mathbf{j})} q_{j_1}\dots q_{j_k} = (q_1\dots q_s)^{2^{s-1}},$$

and this, together with (6.23) and (6.24), completes the proof of (6.10). □

Proof of Lemma 3.10. We take $M = 3$ in Proposition 6.2. Since $p \equiv 1 \pmod 6$, then $q_1 = 2$ gives $(p+q_1)/3 \equiv 1 \pmod 2$, so (6.9) becomes the case $s = 1$ of (3.8). Next, since $x^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$ for any integer x with $p \nmid x$, it suffices to note that $2^{s-1} \equiv (-1)^{s-1} \pmod 3$ in order to see that (6.10) becomes (3.8) for $s \geq 2$. □

Proof of Lemma 3.11. Now let $M = 6$. Then (6.9) immediately gives (3.9). For $s \geq 2$ we note that

$$\frac{1}{6}2^{s-1}\varphi(p^\alpha) = \frac{1}{3}2^{s-2}\varphi(p^\alpha) \equiv \frac{1}{3}(-1)^{s-2}\varphi(p^\alpha) = \frac{1}{3}(-1)^s\varphi(p^\alpha) \pmod{\varphi(p^\alpha)}.$$

This completes the proof of Lemma 3.11. □

7. Computations

In this section we deal with various computational issues arising in this paper. These are, in particular, the computation of Jacobi primes, computing Gauss factorials and their orders, and factoring generalized Fermat numbers. We also give explicit solutions of the congruences (2.5) and (2.6) for two specific examples, while the solutions for all Jacobi primes listed in Tables 7.1, 7.4 and 7.5 are deposited at [6] and [14].

7.1. **Finding Jacobi primes.** We recall that, by (4.9), a prime $p \equiv 1 \pmod 3$ is a Jacobi prime of level ℓ if and only if $\mathrm{ord}_p(r) = 2^\ell$, where r is as defined in (4.5). In Proposition 4.7 we saw that the level-0 (or standard) Jacobi primes are exactly the primes of the form $p = 27X^2 + 27X + 7$, and these are easy to compute. Because of their relative abundance we list only those with $p < 10^5$ in Table 7.1, along with the integers a and b from the expression $p = a^2 + 3b^2$, $a \equiv -1 \pmod 3$ and $b > 0$, and with the relevant orders defined in (4.2).

Table 7.1. Standard Jacobi primes $p < 10^5$, with a, b and orders.

p	a	b	$\gamma_1^3(p)$	$\gamma_1^6(p)$	p	a	b	$\gamma_1^3(p)$	$\gamma_1^6(p)$
7	2	1	3	1	9241	83	28	3	2^2
61	−7	2	3	$3\cdot 2^2$	10267	−88	29	3	$3\cdot 2$
331	−16	5	3	$3\cdot 2$	13669	101	34	1	$3\cdot 2^2$
547	20	7	3	$3\cdot 2$	23497	−133	44	3	2^2
1951	38	13	3	3	25117	137	46	1	$3\cdot 2^2$
2437	−43	14	3	2^2	55897	−205	68	1	$3\cdot 2^2$
3571	−52	17	1	$3\cdot 2$	60919	−214	71	3	$3\cdot 2$
4219	56	19	1	$3\cdot 2$	74419	236	79	3	1
7351	74	25	3	3	89269	−259	86	1	$3\cdot 2^2$
8269	−79	26	3	$3\cdot 2^2$	92401	263	88	3	2^2

To compute the nonstandard Jacobi primes, we first recall from Proposition 4.7 that there are none of level 1 and that the only level-2 Jacobi prime is $p = 13$.

Hence we may restrict our attention to $\ell \geq 3$, and since by (4.9) we have $r^{2^\ell} \equiv 1 \pmod{p}$, this means that $2^3 \mid p-1$, and thus $p \equiv 1 \pmod{24}$; this is a significant restriction as it reduces the required number of calculations by about 75%. Our main tool will be the unique expansion

$$p = a^2 + 3b^2, \quad a \equiv -1 \pmod{3}, \quad b > 0, \tag{7.1}$$

which was already used in Section 4. We now proceed in two separate stages:

1. To find Jacobi primes of levels $3 \leq \ell < D$ for some parameter D to be determined later, we begin with a few easy observations. First, it is clear that a and b in (7.1) have to be of opposite parity since otherwise p would be even. If a were even and b odd, then we would have $a^2 + 3b^2 \equiv 3 \pmod{4}$, which contradicts $p \equiv 1 \pmod{24}$. Hence a is odd and b is even. But furthermore, if $b \equiv 2 \pmod{4}$, then $3b^2 \equiv 4 \pmod{8}$, while $a^2 \equiv 1 \pmod{8}$; this again leads to a contradiction, and so $b \equiv 0 \pmod{4}$, i.e., $b \equiv 0, 4$ or $8 \pmod{12}$. On the other hand, since $3 \nmid a$ in addition to a being odd, we have $a \equiv 1, 5, 7$ or $11 \pmod{12}$. In our first algorithm, described below, we loop through positive integers a and b in these residue classes and define p by (7.1) without checking for primality until needed later in the algorithm, an approach suggested by Yves Gallot. However, we eliminate pairs (a, b) with $\gcd(a, b) > 1$ to avoid cases where p is trivially composite. We also use (7.1) to establish obvious search limits. All this gives rise to the following algorithm.

Algorithm 7.2. To find Jacobi primes $p \leq 10^C$ with levels $3 \leq \ell < D$:

(a) Let (A, B) run through the 12 pairs $\{1, 5, 7, 11\} \times \{0, 4, 8\}$.
(b) Let $a \equiv A \pmod{12}$ run from A to $10^{C/2}$.
(c) Let $b \equiv B \pmod{12}$ run from B to $\sqrt{(10^C - a^2)/3}$.
(d) Let $p := a^2 + 3b^2$.
(e) Let $r := 2a, -a + 3b$ or $-a - 3b$, according as $B = 0, 4$ or 8. If $A = 1$ or 7, replace a by $-a$.
(f) If $r \neq 1$, $r^{2^{D-1}} \equiv 1 \pmod{p}$ and p is prime, then p is a Jacobi prime of level $< D$.
(g) The smallest ℓ, $3 \leq \ell \leq D$, for which $r^{2^\ell} \equiv 1 \pmod{p}$ is the level.

We note that this algorithm lends itself to computing the twelve cases of (a) in parallel. For each of these cases the choices in (e) are fixed. Furthermore, we note that checking the gcd in (c) is very fast, and the modular exponentiation in (f) is reasonably fast. The expensive primality testing then needs to be rarely done. In (f), $r = 1$ can occur only in the cases $(A, B) = (1, 8)$ and $(11, 4)$, and needs to be checked only there.

2. To find Jacobi primes with levels $\ell \geq D$, we use a more direct approach, noting that by (4.9) and an argument made earlier, we may restrict our attention to primes $p \equiv 1 \pmod{3 \cdot 2^D}$.

Algorithm 7.3. To find Jacobi primes $p \leq 10^C$ with levels $\ell \geq D$:

(a) Let the integer p run from $3 \cdot 2^D$ in increments of 2^D to 10^C.
(b) Test p for primality.
(c) Find the unique integers a, b defined by (7.1).
(d) Let $r := 2a, -a + 3b$ or $-a - 3b$, according as $b \equiv 0, 1$ or $2 \pmod{3}$.
(e) If $\operatorname{ord}_p(r) = 2^\ell$, then p is a Jacobi prime of order ℓ.

The parameter D determines the balance between the two algorithms. We found that for $C = 14$ a reasonable choice was $D = 20$. However, since the computational aspects have not been the main focus of this paper, we did not attempt to optimize this balance. Also, for maximal ease of use during this work, we implemented the algorithms in the computer algebra package MAPLE and ran it on a desktop computer. We used built-in MAPLE routines for modular exponentiation in Algorithm 7.2(f), for primality testing in Algorithm 7.2(f) and 7.3(b), for solving the diophantine equation in 2(c), and for finding the orders in 2(e). The results of these computations are recorded in Table 7.4 and, with fewer details, in Table 7.5.

TABLE 7.4. Nonstandard Jacobi primes $p < 10^6$, with a, b, r and orders.

p	a	b	r	$\mathrm{ord}_p r$	$\gamma_1^3(p)$	$\gamma_1^6(p)$
13	-1	2	-5	2^2	$3 \cdot 2^2$	$3 \cdot 2^2$
97	-7	4	19	2^5	$3 \cdot 2^5$	$3 \cdot 2^4$
193	-1	8	-23	2^5	$3 \cdot 2^5$	$3 \cdot 2^4$
409	-19	4	31	2^3	2^3	$3 \cdot 2$
769	-1	16	49	2^7	$3 \cdot 2^7$	$3 \cdot 2^6$
2593	-49	8	25	2^4	2^4	$3 \cdot 2^3$
4729	29	36	58	2^3	2^3	2
6481	41	40	79	2^4	2^4	$3 \cdot 2^3$
12289	-1	64	193	2^{11}	$3 \cdot 2^{11}$	2^{10}
15361	119	20	-179	2^4	$3 \cdot 2^4$	$3 \cdot 2^3$
55681	191	80	-431	2^6	$3 \cdot 2^6$	$3 \cdot 2^5$
331777	95	328	889	2^{10}	$3 \cdot 2^{10}$	$3 \cdot 2^9$
417793	641	48	1282	2^{13}	2^{13}	2^{12}
737281	-841	100	1141	2^{11}	2^{11}	$3 \cdot 2^{10}$
786433	-1	512	-1535	2^{17}	$3 \cdot 2^{17}$	$3 \cdot 2^{16}$

TABLE 7.5. Nonstandard Jacobi primes p, $10^6 < p < 10^{14}$, with levels ℓ and L.

p	ℓ	L	p	ℓ	L	p	ℓ	L
2752513	17	16	860301577	3	0	1136051159041	16	15
6684673	17	16	1380974593	20	19	1618173493249	19	18
8650753	16	15	1845657601	14	13	3788060491777	25	24
36175873	18	17	3221225473	28	27	3893453733889	9	8
69206017	21	20	3255828481	20	19	4713049675777	9	8
75079681	13	12	3281584129	14	13	4754528796673	30	29
155344897	10	9	8531146753	11	10	6597069766657	40	39
270532609	20	19	206158430209	35	34	9748709033473	9	8
435486721	16	15	460794822529	7	6	25177098289153	33	32
824717353	3	1	844734922753	21	20	69803955978241	31	30

7.2. **Computing Gauss factorials and their orders.** Since Gauss factorials (including "usual" factorials) and their orders play an important part in this paper,

it is also interesting to know the values of $\gamma_1^{(3)}(p)$ (see (4.4) and Definition 4.1) as well as $\gamma_1^{(6)}(p)$ and the related level L; see (4.7).

First we note that the computational effort required to obtain the Gauss factorial (in fact, the usual factorial) $\frac{p-1}{3}! \pmod p$ is vastly reduced by using the congruence (4.14), since the integers u are equally easy to compute from (7.1) as the integers r. It therefore suffices to compute $\frac{p-1}{6}! \pmod p$. While for small and moderate-sized primes p this is easily feasible by straightforward multiplication and reduction using MAPLE, it becomes prohibitively expensive for about $p > 10^{10}$ (however, see a discussion about relevant computational strategies in [12, p. 104ff.]). For these larger primes we used a special and very fast program which Yves Gallot kindly made available to us. On a single core of a desktop computer, $\frac{p-1}{6}! \pmod p$ was found in just over 2 minutes for $p = 206\,158\,430\,209$, and in just over 19 hours for $p = 69\,803\,955\,978\,241$. The corresponding orders were then again computed using the `order` routine in MAPLE; the results are recorded in Tables 7.4 and 7.5.

7.3. **Factoring generalized Fermat numbers.** To apply Theorems 5.6 and 5.8, we need to know the prime factors of $p-1$, $p+1$ and $p^{2^j}+1$ for as many $j \ge 1$ as possible, where p is a Jacobi prime. Given the moderate sizes of the Jacobi primes under consideration, factoring $p-1$, $p+1$, p^2+1 and p^4+1 presents no problem and is quickly done with MAPLE. For $j \ge 3$ we dealt with it in several steps:

1. We used the `ifactor` routine in MAPLE with the `easy` option to quickly and efficiently find small factors. Numerous smaller generalized Fermat numbers were completely factored in this way, along with some larger ones, when all prime factors except one happened to be small.

2. Following this, and in some cases independent of Step 1, we used the `factor` routine in Sage [31] to find further prime factors of small and moderate size.

3. In conjunction with Steps 1 and 2 we also consulted the published and online resources [3, 15, 30], verifying our factorizations and finding further factors.

4. Remaining composite cofactors were then subjected to the Elliptic Curve Method in the GMP-ECM implementation [16].

5. Finally, if after a reasonable effort (depending on the size of the number to be factored) the ECM failed for integers up to 166 decimal digits, we used the Number Field Sieve in the CADO-NFS implementation [4], which was always successful.

6. Tables of all prime factors obtained in Steps 1–5 are deposited at [6] and [14]. A small subset can be found in Table 7.7.

In what follows, we refer to the primes $q_i (\equiv -1 \pmod 3)$ in parts (c) of Theorem 5.6 and Theorem 5.8 as *support primes* of a given Jacobi prime p. The prime $q = 2$ is a special case as it is always a support prime in the case of denominator 3, but never in the case of denominator 6; see Remark 5.9.

Although the ECM is well suited to find reasonably small factors of large integers, we made concentrated factorization efforts, as described above, only for those exponents j that were "adjacent" to those for which we already had a complete factorization. Still, it is interesting to note that there are easily obtained complete factorizations of $p^{2^j}+1$ for $p = 97$, $j = 9$, and for $p = 3\,221\,225\,473$ with $j = 8$ and $j = 9$. In this last case, for $j = 8$, the corresponding generalized Fermat number has a 2429-digit support prime, which therefore contributes to appropriate solutions of (2.5) and (2.6). It is also worth mentioning that

$$\tfrac{1}{2}\big(331^{2^8}+1\big), \quad \tfrac{1}{2}\big(2\,752\,513^{2^4}+1\big), \quad \text{and} \quad \tfrac{1}{2}\big(6\,684\,673^{2^5}+1\big)$$

are all primes, with 645, 103 and 219 digits, respectively, but none of them are support primes, which follows from their definitions. Some notable factorizations, achieved with the ECM and the NFS, are summarized in Table 7.6.

TABLE 7.6. Numbers of digits of factors of some $p^{2^j}+1$.

p	j	C	P	M	p	j	C	P	M
1 951	6	157	**72**, 85	N	331 777	5	170	**51**, **119**	E
2 437	6	166	67, **99**	N	737 281	7	702	**43**, **660**	E
4 219	6	156	**77**, **80**	N	75 079 681	5	197	**43**, 155	E
25 117	6	197	**43**, **154**	E	460 794 822 529	4	151	75, 77	N
55 681	6	293	**44**, **249**	E	1 136 051 159 041	4	154	**76**, 78	N

Here the heading C indicates the number of digits of a composite cofactor, after smaller factors of $p^{2^j}+1$ have been removed; P indicates the number of digits of the prime factors found, with support primes in bold, and M indicates the method used, namely the E(CM) or the N(FS).

7.4. **Examples.** In this subsection we consider two specific examples, similar to Examples 2.2 and 2.3, but now with the benefit of having Theorems 5.6 and 5.8 at our disposal. These examples were chosen for their very different natures from each other. For easy reference we begin by giving the complete factorizations of the relevant generalized Fermat numbers in Table 7.7.

TABLE 7.7. Complete factorizations of $\frac{1}{2}(p^{2^j}+1)$ for $p=331$ and $p=55681$.

p	j	factors
331	1	**29** · **1889**
	2	**17** · **41** · 8610913
	3	72673 · **14927201** · **66411377**
	4	**36833** · 1361089 · **1776833** · **6271510529** · **18581275406849**
	5	**30977** · **26705372033** · **22651529502630467180252834145433 7** ·**11500859147495413276035382763489 93**
	6	**641** · **3329** · **4481** · **51713** · 31644673 · **1024640129** · p_{79} ·**20973135548033** · 20115947936290688630487737653815350 1697
	7	**257** · 10753 · 15751388929 · **345807320321** · 43197116304176641 · p_{278}
	8	p_{645}
55681	1	373 · 4155997
	2	**41** · 3001 · 321553 · **121477457**
	3	**17** · **12075324422351249** · 225049724837235459937
	4	794655492577 · p_{64}
	5	**257** · **610817** · **476600704619911891073** · 5411527113131759318593 ·**49403957554237215440934649 7** · p_{75}
	6	769 · 1153 · 84481 · **65298013540910483767858261037118325206398849** · $\mathbf{p_{249}}$

Example 7.8. Let $p = 331$, a standard Jacobi prime, i.e., $\ell = 0$. Its support primes can be found in the factorizations $p-1 = 2\cdot 3\cdot 5\cdot 11$, $p+1 = 2^2\cdot 83$, and in the relevant entries (marked in bold) in Table 7.7. None of the odd support primes occur to a power higher than 1.

(a) We begin with the easier case of denominator 6, i.e., Theorem 5.8. Since we have complete factorizations of $p^{2^j}+1$ for all $j \le 8$, we can give complete solutions for all $2 \le s \le 9$, augmented by results for $s = 0$ and $s = 1$.

• $s = 0$: By computation (Table 2.1), $n = p = 331$ is not a solution of (2.6).

• $s = 1$: By Proposition 5.16(i), the only possible solutions of (2.6) are $n = pq$, with $q \in Q_2 := \{5, 11, 29, 83, 1889\}$. However, computations show that none of these is a solution. (For q up to 83, see Table 2.1).

• $s = 2$: The relevant support primes are the factors of $(p-1)(p+1)(p^2+1)$ that are $\equiv -1 \pmod 6$, namely the elements of Q_2. Then exactly the $\binom{5}{2} = 10$ integers $n = 331\, q_1q_2$, with $q_1, q_2 \in Q_2$, are solutions of (5.5). Of these, computations show that the following are also solutions of (2.6): $331\cdot 29\cdot 83$, $331\cdot 29\cdot 1889$, $331\cdot 83\cdot 1889$.

• $s = 3$: The support primes are now the elements of $Q_3 := Q_2 \cup \{17, 41\}$, so the solutions of (5.5) are the $\binom{7}{3} = 35$ integers $n = 331\, q_1q_2q_3$, with $q_1, q_2, q_3 \in Q_3$. Among these, the following turn out to be solutions of (2.6): $331\cdot 5\cdot 11\cdot 17$, $331\cdot 5\cdot 11\cdot 29$, $331\cdot 5\cdot 11\cdot 41$, $331\cdot 5\cdot 11\cdot 83$, and $331\cdot 5\cdot 11\cdot 1889$.

• $s = 4, \ldots, 9$: Continuing as above, for each s we easily obtain all solutions of (5.5) and by computations the subsets of solutions of (2.6). Table 7.9 gives a summary, with $\#q_j$ showing the numbers of relevant support primes, and "# digits" the numbers of digits of the smallest and largest solutions of (2.6).

TABLE 7.9. Numbers of solutions of (5.5) and (2.6), $p = 331$.

s	$\#q_j$	(5.5)	(2.6)	# digits	s	$\#q_j$	(5.5)	(2.6)	# digits
2	5	10	3	6–8	6	17	12 376	4 362	11–110
3	7	35	5	6–8	7	23	245 157	81 690	15–123
4	9	126	41	8–20	8	25	1 081 575	360 381	17–135
5	13	1 287	411	13–47	9	25	2 042 975	680 973	20–142

(b) We now consider the case of denominator 3, i.e., Theorem 5.6. For a summary of the differences between the two cases, see again Remark 5.9. In particular, $q = 2$ is now a support prime.

• $s = 0$: By Table 7.1, $\gamma_1^3(331) = 3$, so $n = p = 331$ is not a solution of (2.5).

• $s = 1$: By Proposition 5.14(a), the only potential solutions of (2.5) are $n = 331\, q$, with $q \in \{5, 11\}$. However, Table 2.1 shows that neither one is actually a solution.

• $s = 2$: The relevant support primes are now the factors of $(p-1)(p+1)$ that are $-1 \pmod 3$, namely the elements of the set $\overline{Q}_2 \cup \{2\}$, where $\overline{Q}_2 := \{5, 11, 83\}$. Then the solutions of (5.2) are the $\binom{3}{2} = 3$ integers $n = 331\, q_1q_2$ with $q_1, q_2 \in \overline{Q}_2$, together with the $3\cdot\binom{3}{1} = 9$ integers $n = 331\cdot 2^\beta q_2$, where $1 \le \beta \le 3$ and $q_2 \in \overline{Q}_2$. Of these 12 solutions of (5.2), only $n = 331\cdot 5\cdot 11$ is also a solution of (2.5).

• $s = 3$: The support primes are the elements of $\overline{Q}_3 \cup \{2\}$, where $\overline{Q}_3 := \overline{Q}_2 \cup \{29, 1889\}$. Also, p^2+1 contributes to the power of 2, which is now 2^4. Hence

TABLE 7.10. Numbers of solutions of (5.2) and (2.5), $p = 331$.

s	$\#q_j$	(5.2)	(2.5)	# digits	s	$\#q_j$	(5.2)	(2.5)	# digits
2	4	12	1	5	7	18	118 456	38 685	14–117
3	6	50	30	5–9	8	24	2 696 727	901 245	14–130
4	8	210	55	8–11	9	26	12 858 725	4 287 960	17–142
5	10	882	420	8–25	10	26	25 741 485	8 578 366	20–150
6	14	10 725	3 501	10–48					

the solutions of (2.5) in this case are exactly the $\binom{5}{3} = 10$ integers $n = 331\, q_1q_2q_3$, with $q_1, q_2, q_3 \in \overline{Q}_3$, together with the $4 \cdot \binom{5}{2} = 40$ integers $n = 331 \cdot 2^\beta q_2q_3$, with $1 \le \beta \le 4$ and $q_2, q_3 \in \overline{Q}_3$. Of the 10 odd solutions of (5.2), 6 turn out to solve (2.5) as well, the smallest one being $n = 331 \cdot 5 \cdot 29 \cdot 83$. Of the 40 even solutions of (5.2), 24 are solutions of (2.5), with $n = 331 \cdot 2 \cdot 5 \cdot 29$ being the smallest.

• $s = 4, \dots, 10$: Once again, we continue as above, determining all solutions of (5.2) for each s and as a subset the solutions of (2.5) by computation. A summary is given in Table 7.10.

Example 7.11. Let $p = 55681$, a nonstandard Jacobi prime of levels $\ell = 6$ and $L = 5$ (see Table 7.4). Its support primes can again be found in the factors of $p - 1 = 2^7 \cdot 3 \cdot 5 \cdot 29$ and $p + 1 = 2 \cdot 11 \cdot 2531$, and in Table 7.7. We note again that p is not 1-exceptional and that none of the odd support primes in the range under consideration occur to a power higher than 1.

(a) We begin with denominator 6. We have complete factorizations of $p^{2^j} + 1$ for all $j \le 6$; we can give complete solutions for all $s \le 7$.

• $s = 0, 1$: By Propositions 5.12, 5.14, respectively, there are no solutions of (2.6).

• $s = 2, 3, 4$: By Theorem 5.8(b) there can be no solutions of (5.5), and thus of (2.6), since $L = 5$.

• $s = 5$: There are 8 support primes, namely the elements of the set $Q_5 := \{5, 11, 17, 29, 41, 2531, 121477457, 12075324422351249\}$. The solutions of (5.5) are therefore exactly the $\binom{8}{5} = 56$ integers $n = 55681\, q_1 \dots q_5$, with $q_j \in Q_5$, $j = 1, \dots, 5$. Computations show that 18 of these are solutions of (2.6) as well, the smallest of which being $n = 55681 \cdot 5 \cdot 11 \cdot 17 \cdot 29 \cdot 41$, an 11-digit integer.

• $s = 6, 7$: As above, Theorem 5.8 and Table 7.7 give all solutions of (5.5). Computations then lead to the solutions of (2.6); see the summary in Table 7.12.

(b) In the case of denominator 3 we need to take the support prime $q = 2$ into account, and in this case we can determine all solutions for $s \le 8$.

• $s = 0, \dots, 5$: By Propositions 5.10 and 5.14 (for $s = 0, 1$, respectively) and Theorem 5.6(b) there can be no solutions of (5.2), and thus of (2.5).

• $s = 6$: There are 9 support primes, namely the elements of $\{2\} \cup Q_5$, with $q = 2$ occurring to the twelfth power. Accordingly, the solutions of (5.2) consist of the $\binom{8}{6} = 28$ odd integers $n = 55681\, q_1 \dots q_6$ with $q_j \in Q_5$, $j = 1, \dots, 6$, along with the $12\binom{8}{5} = 672$ even integers $n = 55681 \cdot 2^\beta q_2 \dots q_6$ with $1 \le \beta \le 12$ and $q_j \in Q_5$, $j = 2, \dots, 6$. Among these, 12 of the odd and 252 of the even solutions turn out to be solutions of (2.5) as well.

• $s = 7, 8$: Once again, we proceed as above and summarize the numbers of solutions in the right half of Table 7.12.

TABLE 7.12. Numbers of solutions of (5.5), (2.6), (5.2) and (2.5), $p = 55681$.

s	$\#q_j$	(5.5)	(2.6)	# digits	s	$\#q_j$	(5.2)	(2.5)	# digits
5	8	56	18	11–36	6	9	700	264	18–39
6	12	924	306	14–84	7	13	12 804	4 320	15–89
7	14	3 432	1 140	19–371	8	15	51 051	17 127	17–379

To check whether solutions of (5.5) or (5.2) are also solutions of (2.6), resp. (2.5), according to the Chinese Remainder Theorem it suffices to compute the relevant Gauss factorials modulo p, since by Lemma 3.3 they are automatically 1 (mod w). This can be done quickly and efficiently with MAPLE, using the congruence (4.9) when appropriate.

Finally, we note that the ratios between the numbers of solutions of (2.6) and (5.5), resp. (2.5) and (5.2), are usually very close to 1/3. For instance, for $p = 331$ and denominator 3 (Table 7.10), this ratio is approximately 0.33347 for $s = 9$ and 0.33325 for $s = 10$. This is related to Remark 5.11(2).

8. FURTHER REMARKS

8.1. **Very large Jacobi primes.** In Table 5 of his well-known book [30], H. Riesel listed primes of the form $p = h \cdot 2^n + 1$. Of particular interest for this paper are those with $h = 3$. In this case the order of $\frac{p-1}{3}!$ modulo p divides $p - 1 = 3 \cdot 2^n$ and therefore must be $3 \cdot 2^\ell$ or 2^ℓ, i.e., p is always a Jacobi prime. Riesel's table has been vastly extended, and the website [1] lists the primes $p = 3 \cdot 2^n + 1$ for the values of n shown in Table 8.1 and in addition six larger n up to the search limit 8 426 000 (as of July, 2014).

TABLE 8.1. Jacobi primes $p = 3 \cdot 2^n + 1$, $n < 10^6$, with $\Delta = n - \ell$.

n	Δ	n	Δ	n	Δ	n	Δ	n	Δ	n	Δ
1	1	30	2	276	2	3168	2	44685	0	213321	0
2	0	36	1	353	0	3189	0	48150	2	303093	1
5	0	41	1	408	1	3912	2	54792	1	362765	0
6	1	66	1	438	1	20909	3	55182	2	382449	0
8	1	189	0	534	1	34350	2	59973	2	709968	1
12	1	201	1	2208	5	42294	2	80190	1	801978	3
18	1	209	0	2816	3	42665	0	157169	0	916773	0

The first ten entries in this list, up to $n = 41$, also appear in Tables 7.4 and 7.5. Up to $n = 3912$, the levels ℓ are easy to compute by way of Algorithm 7.3. For larger n, we proceed as follows: (i) When n is even, say $n = 2m$, then $a = -1$, $b = 2^m$, and by (4.13) we have $r = 1 + 3 \cdot (-2)^m$. (ii) When n is odd, we use the `qfbsolve` routine in Sage [31] to find a positive solution (a, b). With the appropriate choice of the sign of a, (4.13) gives r. (iii) In both cases we use modular exponentiation to compute $r^{2^{n-10}} \pmod p$, and then square the result repeatedly modulo p until 1 (mod p) is reached within Δ steps from n; see Table 8.1.

8.2. **Heuristics for the number of solutions.** As we have seen in Section 6.4, our ability to find solutions of the congruences (2.5) and (2.6) depends to a large extent on the level ℓ of the Jacobi prime $p \mid n$, on our ability to factor $p-1$ and the generalized Fermat numbers $F_k(p)$ for $0 \le k \le s-2$ (resp. $0 \le k \le s-1$, where s is as in (2.4)), and on the number of primes $q \equiv -1 \pmod 3$ among the prime divisors of these $F_k(p)$. This gives rise to the following question: Given a Jacobi prime p, are there always integers $n = pq_1 \dots q_s$ that solve the congruences (2.5) or (2.6)? We will show heuristically that this is always the case and that, in fact, we can expect infinitely many such solutions of (2.5) and of (2.6).

We begin with the well-known fact that the normal order of the number $\omega(n)$ of distinct prime factors of an integer n is $\log\log n$ (see, e.g., [20, p. 356]). We now make the obviously unproven assumptions that the factors of a generalized Fermat number $F_k(p) = p^{2^k}+1$ behave like those of a random integer and that, on average, half of the prime divisors of $F_k(p)$ lie in the residue class of $-1 \pmod 3$. Then we can expect that the number of prime divisors $q \equiv -1 \pmod 3$ of $F_k(p)$ is roughly

$$\frac{1}{2}\log\log F_k(p) > \frac{1}{2}\log(2^k \log p) > \frac{\log 2}{2}\cdot k. \tag{8.1}$$

Next we use the fact that apart from 2, no two generalized Fermat numbers with a fixed base p have a common factor; see, e.g., [22, p. 149].

Combining this with the estimate (8.1), we can expect roughly

$$\frac{\log 2}{2}(1+2+\dots+(s-2)) = \frac{\log 2}{4}(s-2)(s-1) \tag{8.2}$$

distinct prime divisors $q \equiv -1 \pmod 3$ of $(p-1)(p+1)\dots(p^{2^{s-2}}+1)$. Based on our assumptions, the number of these prime divisors will therefore soon exceed $s \ge \ell$, which by Theorem 5.6 is necessary and sufficient for (5.2) to have a solution. As we let s increase, the combinatorial arguments of Section 6.4 show that we can expect the number of solutions to increase quite rapidly, and as we have seen, we can expect about 1/3 of these solutions to also be solutions of (2.5).

We can make the same argument for the solutions of (5.5) and (2.6), with only the small change of replacing s by $s+1$ in (8.2).

8.3. **Closing remarks.** This paper has been about solutions of the congruence (2.5) and (2.6) for integers n exclusively of the form (2.4), i.e., $n = p^\alpha w$, with $p \equiv 1 \pmod 3$ being the only prime factor in this residue class. In Remark 2.4 we noted that $\alpha = 2$ is extremely rare when n is a solution, with $p = 13$ being the only prime up to 10^{14} for which this can occur, and that there is no prime in this range for which $\alpha > 2$ is possible. This is in stark contrast to the case where n has two distinct primes congruent to 1 (mod 3), as the following result shows.

Proposition 8.2. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2}$, where $p_1 \equiv p_2 \equiv 1 \pmod{12}$ are distinct primes that are sextic residues of each other. Then*

$$\left(\tfrac{n-1}{6}\right)_n ! \equiv 1 \pmod n$$

for all integers $\alpha_1, \alpha_2 \ge 1$.

Since this is not central to the main topic of this paper, we only mention that the proof is based on a special case of a closed-form congruence in Lemma 2 of [9] that is of a similar nature (although different in detail) to the congruences in Section 3. A similar, but simpler, result can also be obtained for the case $M = 3$.

In both cases there are infinitely many pairs (p_1, p_2) that provide solutions; in the case of Proposition 8.2 they can be found by searching for simultaneous solutions of reciprocal pairs of congruences:

$$p_1^{(p_2-1)/6} \equiv 1 \pmod{p_2}, \qquad p_2^{(p_1-1)/6} \equiv 1 \pmod{p_1}.$$

The five smallest solutions by size of their product $n = p_1 p_2$ are $13 \cdot 1117$, $61 \cdot 241$, $37 \cdot 433$, $13 \cdot 1741$, and $13 \cdot 1873$.

Acknowledgments

The authors would like to thank Douglas Staple for his invaluable help with factoring some difficult integers, François Morain for verifying the primality of a 2429-digit factor, and Yves Gallot for his help with calculating large factorials modulo p.

References

[1] R. Ballinger and W. Keller, List of primes $k.2^n + 1$ for $k < 300$. Updated July 2014. `http://www.prothsearch.net/riesel.html`.

[2] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998. MR1625181 (99d:11092)

[3] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff Jr., *Factorizations of $b^n \pm 1$: $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*, Contemporary Mathematics, vol. 22, American Mathematical Society, Providence, R.I., 1983. MR715603 (84k:10005)

[4] CADO-NFS (Crible Algébrique: Distribution, Optimisation - Number Field Sieve). Available at `http://cado-nfs.gforge.inria.fr`.

[5] C. K. Caldwell and T. Komatsu, *Powers of Sierpiński numbers base B*, Integers **10** (2010), A36, 423–436, DOI 10.1515/INTEG.2010.036. MR2684132 (2011j:11010)

[6] J. B. Cosgrave, `http://www.johnbcosgrave.com/computations.php`

[7] J. B. Cosgrave and K. Dilcher, *Extensions of the Gauss-Wilson theorem*, Integers **8** (2008), A39, 15. MR2472057 (2009k:11004)

[8] J. B. Cosgrave and K. Dilcher, *The multiplicative orders of certain Gauss factorials*, Int. J. Number Theory **7** (2011), no. 1, 145–171, DOI 10.1142/S179304211100396X. MR2776014 (2012c:11003)

[9] J. B. Cosgrave and K. Dilcher, *An introduction to Gauss factorials*, Amer. Math. Monthly **118** (2011), no. 9, 812–829, DOI 10.4169/amer.math.monthly.118.09.812. MR2854003 (2012j:11009)

[10] J. B. Cosgrave and K. Dilcher, *The Gauss-Wilson theorem for quarter-intervals*, Acta Math. Hungar. **142** (2014), no. 1, 199–230, DOI 10.1007/s10474-013-0357-1. MR3158860

[11] J. B. Cosgrave and K. Dilcher, *The multiplicative orders of certain Gauss factorials, II*, Funct. Approx. Comment. Math. **54** (2016), no. 1, 73–93, DOI 10.7169/facm/2016.54.1.7. MR3477736

[12] R. E. Crandall, *Topics in advanced scientific computation*, Springer-Verlag, New York; TELOS. The Electronic Library of Science, Santa Clara, CA, 1996. MR1392472 (97g:65005)

[13] L. E. Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality*, Chelsea Publishing Co., New York, 1966. MR0245499 (39 #6807a)

[14] K. Dilcher, `http://hdl.handle.net/10222/71449`.

[15] `http://factordb.com/`.

[16] GMP-ECM (Elliptic Curve Method for Integer Factorization), available at `https://gforge.inria.fr/projects/ecm/`.

[17] P. Gaudry, A. Kruppa, F. Morain, L. Muller, E. Thomé, and P. Zimmermann, `cado-nfs`, An Implementation of the Number Field Sieve Algorithm. Release `1.0`, available from `http://cado-nfs.gforge.inria.fr/`.

[18] H. W. Gould, *Combinatorial identities*: *A standardized set of tables listing 500 binomial coefficient summations*, Henry W. Gould, Morgantown, W.Va., 1972. MR0354401 (50 #6879)

[19] T. A. Gulliver, *Self-reciprocal polynomials and generalized Fermat numbers*, IEEE Trans. Inform. Theory **38** (1992), no. 3, 1149–1154, DOI 10.1109/18.135659. MR1162838 (93h:11135)
[20] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., The Clarendon Press, Oxford University Press, New York, 1979. MR568909 (81i:10002)
[21] R. H. Hudson and K. S. Williams, *Binomial coefficients and Jacobi sums*, Trans. Amer. Math. Soc. **281** (1984), no. 2, 431–505, DOI 10.2307/2000071. MR722761 (85m:11092)
[22] M. Křížek, F. Luca, and L. Somer, *17 lectures on Fermat numbers*: *From number theory to geometry*, with a foreword by Alena Šolcová, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 9, Springer-Verlag, New York, 2001. MR1866957 (2002i:11001)
[23] D. H. Lehmer, *The distribution of totatives*, Canad. J. Math. **7** (1955), 347–357. MR0069199 (16,998i)
[24] Maple, a computer algebra system. Available at `http://www.maplesoft.com/products/maple/`.
[25] T. Müller, *A generalization of a theorem by Křížek, Luca, and Somer on elite primes*, Analysis (Munich) **28** (2008), no. 4, 375–382, DOI 10.1524/anly.2008.0922. MR2477353 (2010a:11013)
[26] T. Müller, *On the Fermat periods of natural numbers*, J. Integer Seq. **13** (2010), no. 9, Article 10.9.5, 12. MR2746253 (2011m:11017)
[27] T. Müller and A. Reinhart, *On generalized elite primes*, J. Integer Seq. **11** (2008), no. 3, Article 08.3.1, 15. MR2429958 (2009h:11008)
[28] OEIS Foundation Inc. (2011), The On-Line Encyclopedia of Integer Sequences. Available at `http://oeis.org`.
[29] P. Ribenboim, *The new book of prime number records*, Springer-Verlag, New York, 1996. MR1377060 (96k:11112)
[30] H. Riesel, *Prime numbers and computer methods for factorization*, 2nd ed., Progress in Mathematics, vol. 126, Birkhäuser Boston, Inc., Boston, MA, 1994. MR1292250 (95h:11142)
[31] SageMath, a free open-source mathematics software system licensed under the GPL. Available at `http://www.sagemath.org/`.

79 Rowanbyrn, Blackrock, County Dublin, A94 FF86, Ireland
E-mail address: `jbcosgrave@gmail.com`

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 4R2, Canada
E-mail address: `dilcher@mathstat.dal.ca`