Acta Math. Hungar., **142 (1)** (2014), 199–230
DOI: 10.1007/s10474-013-0357-1
First published online September 18, 2013

THE GAUSS–WILSON THEOREM FOR QUARTER-INTERVALS

J. B. COSGRAVE[1] and K. DILCHER[2,*]

[1]79 Rowanbyrn, Blackrock, County Dublin, Ireland
e-mail: jbcosgrave@gmail.com

[2]Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 4R2, Canada
e-mail: dilcher@mathstat.dal.ca

(Received January 22, 2013; revised April 2, 2013; accepted April 2, 2013)

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. It is the purpose of this paper to study the multiplicative orders of the Gauss factorials $\left\lfloor \frac{n-1}{4} \right\rfloor_n !$ for odd positive integers n. The case where n has exactly one prime factor of the form $p \equiv 1 \pmod 4$ is of particular interest, as will be explained in the introduction. A fundamental role is played by p with the property that the order of $\frac{p-1}{4}!$ modulo p is a power of 2; because of their connection to two different results of Gauss we call them Gauss primes. Our main result is a complete characterization in terms of Gauss primes of those n of the above form that satisfy $\left\lfloor \frac{n-1}{4} \right\rfloor_n ! \equiv 1 \pmod n$. We also report on computations that were required in the process.

1. Introduction

The celebrated 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 positive integers N and n let $N_n!$ denote the product

$$N_n! = \prod_{\substack{1 \leqq j \leqq N \\ \gcd(j,n)=1}} j, \tag{1.1}$$

which in previous papers (see, e.g., [5]) we called a *Gauss factorial*. With this notation the Gauss–Wilson theorem states that for any integer $n \geqq 2$

* Corresponding author. Research supported in part by the Natural Sciences and Engineering Research Council of Canada.

Key words and phrases: Wilson's theorem, Gauss' theorem, factorial, congruence.
Mathematics Subject Classification: primary 11A07, secondary 11B65.

we have

$$(n-1)_n! \equiv \begin{cases} -1 \pmod{n} & \text{for } n = 2, 4, p^\alpha, \text{ or } 2p^\alpha, \\ 1 \pmod{n} & \text{otherwise,} \end{cases} \tag{1.2}$$

where p is an odd prime and α is a positive integer. For references, see [8, p. 65].

It is the purpose of this paper to study certain aspects of the Gauss factorial

$$\left(\frac{n-1}{M}\right)_n ! \pmod{n}, \tag{1.3}$$

where $M \geqq 2$ and $n \equiv 1 \pmod{M}$ are positive integers. The case $M = 2$ was treated by Mordell [12] for odd primes $n = p$, and the authors [2] gave a complete description of the multiplicative orders of $\left(\frac{n-1}{2}\right)_n!$ modulo n for odd n, and also for $\left\lfloor \frac{n-1}{2} \right\rfloor_n!$ when n is even. Further work by the authors [5] shows that the Gauss factorial (1.3) is always congruent to 1 modulo n when n has at least three distinct prime factors congruent to 1 $\pmod{M}$, and that the multiplicative order of (1.3) modulo n is a divisor of M when n has at least two distinct prime factors congruent to 1 $\pmod{M}$. We therefore know a great deal about Gauss factorials in these two cases.

Of the two remaining cases, very little can be said when n has no prime factor congruent to 1 $\pmod{M}$. However, when n has exactly one such prime factor, a very rich structure and strong and pleasing partial results emerge. This case was already explored in [4] when n is a prime power. While in that paper we paid special attention to the cases $M = 3, 4$ and 6, it turns out that there are substantial differences between these cases and all other M. These differences come from the fact that $\varphi(M) = 2$ only for $M = 3, 4$ and 6, and thus any prime $p > 3$ satisfies $p \equiv \pm 1 \pmod{M}$. Furthermore, the case $M = 4$ is fundamentally different from $M = 3$ and 6. In this paper we will be dealing exclusively with $M = 4$; the cases $M = 3$ and 6 will be the subject of a separate paper. We mention in passing that Gauss factorials for $M = 4$ and $M = 3$ have led to some surprising congruences [3] extending Gauss's Theorem 1 below and a related theorem of Jacobi.

To motivate the main purpose of this paper, let us consider the following question: For which integers $n \equiv 1 \pmod{4}$ do we have

$$\left(\frac{n-1}{4}\right)_n ! \equiv 1 \pmod{n}? \tag{1.4}$$

Obviously, this holds for $n = 5$. The next such integers are $n = 205$, 725, 1025, and 1105, with a total of 37 109 up to 10^6. What all these moduli, except $n = 5$, have in common is that they have at least two distinct prime

factors that are congruent to 1 (mod 4). One might therefore be led to conjecture that this is true in general.

However, (1.4) does have solutions with $n \equiv 1 \pmod 4$, and n having only one prime factor $p \equiv 1 \pmod 4$. Such solutions are exceedingly rare, and indeed there are only three up to 10^{20}; see Table 1.

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

Table 1: The 3 smallest solutions of (1.4), $p \equiv 1 \pmod 4$

One of the main results of this paper is the complete characterization of all such integers, some of which are extremely large, as we shall see. In fact, apart from the above three solutions of (1.4) (with $n \equiv 1 \pmod 4$ and a single prime factor $p \equiv 1 \pmod 4$) the least other solution known to us has 155 decimal digits.

In Section 2 we introduce the concepts of a *Gauss prime* and the *support prime powers* of such primes. 46817 and 652081 (in Table 1) are examples of Gauss primes. These notions are fundamental to understanding the above three (indeed all) solutions and in obtaining the desired characterization in Sections 3, with the proofs given in Sections 4 and 5. Some relevant computations are discussed in Section 6, and we conclude this paper with some further remarks in Section 7.

2. Gauss primes

In this section we will restrict our attention to the case where $n = p \equiv 1 \pmod 4$ is a prime. Then the Gauss factorial on the left of (1.4) becomes an ordinary factorial. Investigating the multiplicative orders of these factorials, that is, $\operatorname{ord}_p\left(\frac{p-1}{4}!\right)$, leads to important results and concepts that will be crucial for later results in this paper. To put this in perspective, we list $\frac{p-1}{4}! \pmod p$ and their multiplicative orders for the first 30 primes $p \equiv 1 \pmod 4$; see Table 2. The orders do not appear to be bounded, as was the case with the half-interval factorials treated in [2]. In fact, for numerous primes p, $\frac{p-1}{4}!$ is a primitive root modulo p, i.e., it has maximal order $p-1$.

An important tool for this section (and also later) is the following classical result of Gauss from 1828; see, e.g., [1, p. 200].

p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order	p	$\frac{p-1}{4}!(p)$	order
5	1	**1**	**97**	20	**32**	197	92	98
13	6	12	101	46	100	229	168	38
17	7	**16**	109	7	27	233	36	116
29	23	7	113	32	28	**241**	130	**16**
37	21	18	137	90	136	**257**	120	**32**
41	13	40	149	23	148	269	258	67
53	26	52	157	145	6	277	221	276
61	19	30	173	40	86	281	157	28
73	18	18	181	3	45	293	69	73
89	22	22	**193**	89	**64**	313	109	312

Table 2: The first 30 *primes* $p \equiv 1 \pmod 4$

THEOREM 1 (Gauss). *Let the prime* $p \equiv 1 \pmod 4$ *be written as* $p = a^2 + b^2$, *and choose the sign of* a *such that* $a \equiv 1 \pmod 4$. *Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p. \tag{2.1}$$

In this section we will mainly be concerned with the case where the order of $\frac{p-1}{4}! \pmod p$ is a power of 2; these instances are highlighted in Table 2. We begin with the smallest cases.

THEOREM 2. *Let* $p \equiv 1 \pmod 4$ *be a prime. Then*

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

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

In other words, $\frac{p-1}{4}!$ *cannot have orders* 1, 2, 4, *or* 8, *with the exception of* $p = 5$.

PROOF. First, suppose that $\frac{p-1}{4}! \equiv \pm 1 \pmod p$ or $\left(\frac{p-1}{4}!\right)^2 \equiv -1 \pmod p$, and let $p = a^2 + b^2$ with a an odd positive integer. Now, by Lagrange's elementary extension of Wilson's theorem we have

$$\left(\frac{p-1}{2}!\right)^2 \equiv -1 \pmod p, \tag{2.2}$$

and so with (2.1) we get

$$(\pm 2a)^2 \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{4}}^2 = \frac{\left(\frac{p-1}{2}!\right)^2}{\left(\frac{p-1}{4}!\right)^4} \equiv \frac{-1}{1} \pmod p. \tag{2.3}$$

But $4a^2 \equiv -4b^2 \pmod p$, and thus (2.3) gives $4b^2 \equiv 1 \pmod p$, or $2b \equiv \pm 1 \pmod p$. Since $0 < b < \sqrt{p}$, it is clear that $2b = p - 1$ is the smallest solu-

tion of this last congruence. However, it is easy to see that the inequality $\frac{p-1}{2} < \sqrt{p}$ implies $p < 6$. This proves (a) and also (b) for $k = 1, 2$.

Next, if $\left(\frac{p-1}{4}!\right)^4 \equiv -1 \pmod{p}$ then, similar to (2.3), we get $2a \equiv \pm 1 \pmod{p}$, and $2a = p - 1$ is the smallest possibility. However, $2a = p - 1$ is impossible since $2a \equiv 2 \pmod{4}$ while $p - 1 \equiv 0 \pmod{4}$. Finally, the condition $\frac{p+1}{2} < \sqrt{p}$ easily gives $p < 2$. This completes the proof. □

The case of order 16 is quite different, as we will now see. The following is the main result of this section.

THEOREM 3. *Let $p \equiv 1 \pmod{4}$ be a prime, and write $p = a^2 + b^2$, with $a, b > 0$. Then*

$$\left(\frac{p-1}{4}!\right)^8 \equiv -1 \pmod{p} \tag{2.4}$$

if and only if $p - 1 = 4ab$.

PROOF. We may choose a to be odd. Then, again from (2.1), we get

$$\frac{\left(\frac{p-1}{2}!\right)^4}{\left(\frac{p-1}{4}!\right)^8} \equiv (\pm 2a)^4 \equiv \left(4a^2\right)\left(-4b^2\right) = -(4ab)^2 \pmod{p}.$$

Hence, using (2.2), we have

$$\left(\frac{p-1}{4}!\right)^{-8} \equiv -(4ab)^2 \pmod{p}. \tag{2.5}$$

First, if $p - 1 = 4ab$, then from (2.5) we immediately get (2.4). On the other hand, suppose that (2.4) holds. Then (2.5) gives $(4ab)^2 \equiv 1 \pmod{p}$, and thus $4ab \equiv \pm 1 \pmod{p}$. First suppose that $4ab \equiv 1 \pmod{p}$ and set

$$4ab = mp + 1. \tag{2.6}$$

Since $p = a^2 + b^2$, $a, b > 0$, we have $0 < 4ab < 4\sqrt{p}\sqrt{p} = 4p$, and thus $1 \leqq m \leqq 3$. Considering (2.6) modulo 4 gives $0 \equiv m + 1 \pmod{4}$, so $m = 3$. But then (2.6) can be rewritten as $4ab - 3\left(a^2 + b^2\right) = 1$ or, reduced modulo 5, $2\left(a^2 + 2ab + b^2\right) \equiv 1 \pmod{5}$, or equivalently $(a + b)^2 \equiv 3 \pmod{5}$, which is impossible.

Suppose, therefore, that $4ab \equiv -1 \pmod{p}$. Then with $4ab = mp - 1$ we see, using a similar estimate as before, that $1 \leqq m \leqq 4$, and furthermore we have $0 \equiv m - 1 \pmod{4}$. This means that $m = 1$ and thus $4ab = p - 1$, which completes the proof. □

While Theorem 3 gives an easy criterion for the order to be 16, we can actually say more, and give an algorithm that produces candidates for the congruence (2.4) to hold. Indeed, the equations $p-1=4ab$ and $p=a^2+b^2$ can be combined to give

$$(a-2b)^2-3b^2=1. \tag{2.7}$$

But this is a Pell equation, i.e., a Diophantine equation of the form $x^2-dy^2=1$, here with $d=3$ and $x=a-2b$, $y=b$. Such an equation has always infinitely many solutions which can be found explicitly; see, e.g., [14, p. 351 ff.]. For $d=3$ the least positive solution is clearly $(x_1,y_1)=(2,1)$. Then all other solutions are given by

$$x_n+y_n\sqrt{3}=\left(2+\sqrt{3}\right)^n$$

(see, e.g., [14, p. 354]). Now, setting

$$x_{n+1}+y_{n+1}\sqrt{3}=\left(x_n+y_n\sqrt{3}\right)\left(2+\sqrt{3}\right)=2x_n+3y_n+(x_n+2y_n)\sqrt{3},$$

we have the recurrence relations

$$x_{n+1}=2x_n+3y_n, \qquad y_{n+1}=x_n+2y_n. \tag{2.8}$$

If we number the positive solutions (a,b) of (2.7) by (a_j,b_j), $j=2,3,\dots$, then from (2.8), with $x_k=a_{k+1}-2b_{k+1}$, $y_k=b_{k+1}$, and solving for a_k, b_k, we immediately obtain $b_k=a_{k-1}$ and

$$a_k=4a_{k-1}-a_{k-2}, \quad a_0=0,\ a_1=1. \tag{2.9}$$

We note in passing that $a_k=U_k(4,1)$, where $U_k(P,Q)$ is the *Lucas function* which has been studied extensively; see, e.g., [18]. We have now obtained

Corollary 1. *A prime $p\equiv 1 \pmod 4$ satisfies the congruence*

$$\left(\frac{p-1}{4}!\right)^8\equiv -1 \pmod p$$

if and only if $p=p_k:=a_{k+1}^2+a_k^2$ for some $k\geqq 1$, where the sequence $\{a_k\}$ is defined by (2.9).

The first few values of a_k and p_k are shown in Table 3.

It is easy to verify that p_k is prime for $1\leqq k\leqq 5$. We then used Maple, and for larger k PARI/GP, to find that p_k is composite for $6\leqq k\leqq 100\,000$, with the exception of the following 14 values of k: 131, 200, 296, 350, 519, 704, 950, 5 598, 6 683, 7 445, 8 775, 8 786, 11 565, 12 483; these were all proven

k	a_k	p_k	prime
1	1	17	yes
2	4	241	yes
3	15	3 361	yes
4	56	46 817	yes
5	209	652 081	yes
6	780	9 082 321	no

Table 3: a_k and p_k for $1 \leqq k \leqq 6$

prime by François Morain [13] with the elliptic curve primality test. In addition we found, again using PARI/GP, that p_k is a probable prime for $k = 13\,536$, $18\,006$, $18\,995$, $48\,773$, and $93\,344$.

REMARK. There is an interesting geometric interpretation of the numbers p_k (prime or composite). The sequence $\{1, 17, 241, 3\,361, 46\,817, 652\,081, \ldots\}$ is listed in [15] as sequence A103772 and is defined as those integers a for which the triangle with sides $(a, a, a-1)$ has integral area.

Theorems 2 and 3 and Corollary 1 are results about the orders of $\frac{p-1}{4}!$ as powers of 2. Primes p with this property will play a special role in later sections; we therefore introduce the following terminology.

DEFINITION 1. Let p be a prime with $p \equiv 1 \pmod 4$. If

$$\operatorname{ord}_p\left(\frac{p-1}{4}!\right) = 2^\ell \qquad \text{for some } \ \ell \geqq 0,$$

we say that p is a Gauss prime of level ℓ.

Theorem 2 shows that $p = 5$ is the only Gauss prime of level 0, while there are none of levels 1, 2 or 3. Gauss primes of level 4 are then characterized by Theorem 3, and Corollary 1 gives a method of finding such primes. Finally, Table 2 shows that there are Gauss primes of level 5 ($p = 97$ and 257) and level 6 ($p = 193$).

This leads to the question of whether there exist Gauss primes of higher levels, and how they can be obtained. An approach to this is given by the following easy consequence of Gauss' binomial coefficient theorem (Theorem 1).

LEMMA 1. *Let $p \equiv 1 \pmod 4$ be a prime, and let $\ell \geqq 4$ be an integer. Then p is a Gauss prime of level ℓ if and only if*

$$(2A)^{2^{\ell-2}} \equiv -1 \pmod p, \tag{2.10}$$

where A is a or b in $p = a^2 + b^2$.

PROOF. For simplicity of notation, we set $w := 2^{\ell-2}$. Once again we use (2.1), to get

$$\frac{\left(\frac{p-1}{2}!\right)^w}{\left(\frac{p-1}{4}!\right)^{2w}} \equiv (\pm 2a)^w \equiv (2a)^w \pmod{p},$$

and with (2.2), using the fact that $4 \mid w$, we have

$$\left(\frac{p-1}{4}!\right)^{2w} \equiv -1 \pmod{p} \quad \text{if and only if} \quad (2a)^w \equiv -1 \pmod{p}.$$

Now note that $a^2 \equiv -b^2 \pmod{p}$, and since $4|w$, we can interchange a and b. This completes the proof. □

It is clear from the proof that an analogue of Lemma 1 could be stated for arbitrary positive integers w with $4|w$; however, this will not be needed here. An easy consequence of this lemma is a statement about Fermat primes. As is well known, the nth Fermat number is defined by

$$F_n := 2^{2^n} + 1, \tag{2.11}$$

and when F_n is prime, it is called a Fermat prime. Only $F_0, \ldots, F_4$ are known to be prime; see, e.g., [16].

COROLLARY 2. *If F_n is a Fermat prime, then for $n \geqq 2$ the multiplicative order of $\big((F_n-1)/4\big)!$ modulo F_n is 2^{n+2}, and thus F_n is a Gauss prime of level $n+2$.*

PROOF. This follows directly from Lemma 1 with $A = 1$ and $w = 2^n$. Indeed, (2.11) trivially becomes $2^{2^n} \equiv -1 \pmod{F_n}$, and then (2.10) gives

$$\left(\frac{F_n-1}{4}!\right)^{2^{n+1}} \equiv -1 \pmod{F_n}.$$

The statement of the corollary now follows. □

Thus, all Fermat primes F_n, $n \geqq 2$, are Gauss primes (with $F_2 = 17$ already listed in Table 3 as p_1). Lemma 1 is also most useful in searching for other Gauss primes since the computationally expensive evaluation of $\frac{p-1}{4}! \pmod{p}$ will be avoided. Another reduction in the amount of computation necessary to search for Gauss primes comes from the fact that a level-ℓ Gauss prime p satisfies $p \equiv 1 \pmod{2^\ell}$. This follows from Definition 1 and the fact that the order of any element divides the group order $p-1$.

With these computational enhancements we searched for Gauss primes of levels ℓ with $5 \leqq \ell \leqq 18$, with $p < 10^{16}$ for $\ell = 5$ and $p < 10^{14}$ for $\ell > 5$. In practice, for each prime $p \equiv 1 \pmod{32}$, we computed the unique positive

a and b in $p = a^2 + b^2$, set $A := a$ or $A := b$, and successively squared $2A$ modulo p, recording those pairs (p, ℓ) for which (2.10) holds, up to a desired search limit.

The results are reported in Table 4. Given the strong structure in the case $\ell = 4$ (Theorem 3 and Corollary 1), it is worth mentioning that we were unable to see any apparent structure for $\ell \geqq 5$.

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

Table 4: All Gauss primes $p < 10^{14}$ ($p < 10^{16}$ for $\ell = 5$)

3. The main results

We now return to the question posed at the end of the Introduction: Characterize those integers $n \equiv 1 \pmod 4$ with exactly one prime factor $p \equiv 1 \pmod 4$ for which $\left(\frac{n-1}{4}\right)_n ! \equiv 1 \pmod n$. As mentioned in the Introduction, the primes $p = 46817$ and $p = 652081$ play a special role in this. We note that these primes are listed in Table 4 as two of the Gauss primes; indeed, we shall see that Gauss primes in general will figure prominently in the desired characterization.

We begin with the special case where $n = p^\alpha$, $p \equiv 1 \pmod 4$ and $\alpha \geqq 1$. This case was studied in great detail in a previous paper [4] by the authors, and we quote the following result from that paper. With p and α as above, we set

$$\gamma_\alpha := \operatorname{ord}_{p^\alpha} \left(\frac{p^\alpha - 1}{4}\right)_{p^\alpha} ! . \tag{3.1}$$

Since clearly

$$\left(\frac{p^\alpha - 1}{4}\right)_{p^\alpha} ! = \left(\frac{p^\alpha - 1}{4}\right)_{p} !, \qquad \alpha = 1, 2, 3, \ldots ,$$

we will use the simpler form on the right-hand side whenever it is appropriate. The successive orders γ_α in (3.1) relate as follows; see Proposition 2.2 in [4].

THEOREM 4. *Let $p \equiv 1 \pmod 4$ be a prime, and for $\alpha \geqq 1$ let γ_α be defined as in (3.1). If $p \equiv 1 \pmod 8$, then*

$$\gamma_{\alpha+1} = p\gamma_\alpha \quad \text{or} \quad \gamma_{\alpha+1} = \gamma_\alpha. \tag{3.2}$$

If $p \equiv 5 \pmod 8$, then

$$\gamma_{\alpha+1} = \begin{cases} p\gamma_\alpha \quad \text{or} \quad \gamma_\alpha & \text{when} \quad \gamma_\alpha \equiv 0 \pmod 4, \\ \dfrac{1}{2}p\gamma_\alpha \quad \text{or} \quad \dfrac{1}{2}\gamma_\alpha & \text{when} \quad \gamma_\alpha \equiv 2 \pmod 4, \\ 2p\gamma_\alpha \quad \text{or} \quad 2\gamma_\alpha & \text{when} \quad \gamma_\alpha \equiv 1 \pmod 2. \end{cases} \tag{3.3}$$

Proposition 2.2 in [4] also specifies under which conditions the first (respectively the second) alternatives in (3.2) and (3.3) hold; however, this will not be needed here. From Theorem 4 we now obtain the following extended version of Theorem 2.

COROLLARY 3. *Let $p \equiv 1 \pmod 4$ be a prime. Then*

(a) $\left(\frac{p^\alpha-1}{4}\right)_p! \equiv 1 \pmod{p^\alpha}$ *only for $p = 5$ and $\alpha = 1$.*

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

PROOF. For $\alpha = 1$, this is just Theorem 2; so we assume that $\alpha > 1$. If $p \equiv 1 \pmod 8$ then, by (3.2), $\gamma_\alpha = 1$, 2, 4 or 8 leads to $\gamma_1 = 1$, 2, 4 or 8, respectively. However, by Theorem 2(a) we have $\gamma_1 = 1$ only for $p = 5$ (a contradiction), while $\gamma_1 = 2$, 4 or 8 are impossible by Theorem 2(b).

When $p \equiv 5 \pmod 8$, we have the following cases; see (3.3):

(i) For $\gamma_\alpha = 4$, the values of $\gamma_1, \gamma_2, \ldots, \gamma_\alpha$ would be $\gamma, \gamma, \ldots, \gamma$, giving $\gamma_1 = \gamma = 4$, which is impossible by Theorem 2(b).

(ii) For $\gamma_\alpha = 2$, the values of $\gamma_1, \gamma_2, \ldots, \gamma_\alpha$ would be $\gamma, \frac{\gamma}{2}, \ldots, \gamma$ or $\frac{\gamma}{2}$, giving $\gamma_1 = \gamma = 2$ or 4, which is again impossible.

(iii) For $\gamma_\alpha = 1$, the values of $\gamma_1, \gamma_2, \ldots, \gamma_\alpha$ would be $\gamma, 2\gamma, \ldots, \gamma$ or 2γ, and the only possibility is $\gamma_1 = 1$. By Theorem 2(a) this holds only for $p = 5$. But 5 belongs to those primes for which the first alternative in (3.3) holds; see [4], Section 2. This is again a contradiction for $\alpha > 1$, and the proof is complete. □

Corollary 3(a) means that we may now restrict our attention to

$$n = p^\alpha w, \qquad \text{with} \quad w = q_1^{\beta_1} \cdots q_r^{\beta_r} \quad (r \geqq 1), \tag{3.4}$$

where $p \equiv 1 \pmod 4$ and $q_1 \equiv \ldots \equiv q_r \equiv -1 \pmod 4$ are distinct primes and $\alpha, \beta_1, \ldots, \beta_r$ are positive integers.

Since the integer n, as defined in (3.4), may not be of the form $n \equiv 1 \pmod 4$, we continue with some remarks concerning an extension of the Gauss factorials $\left(\frac{n-1}{4}\right)_n!$, and more generally $\left(\frac{n-1}{M}\right)_n!$. We already mentioned in the Introduction that in [2] we obtained, in addition to results on $\left(\frac{n-1}{2}\right)_n!$ for odd n, also meaningful results for $\left\lfloor\frac{n-1}{2}\right\rfloor_n!$ when n is even. Similarly, in [4] we obtained results for $\left\lfloor\frac{p^\alpha-1}{4}\right\rfloor_p!$ when $p \equiv -1 \pmod 4$ and $\alpha \geqq 1$ that are completely analogous to the "natural" case $\left(\frac{p^\alpha-1}{4}\right)_p!$ when $p \equiv 1 \pmod 4$.

With all this in mind, we extend the congruence (1.4) and ask for which n, as defined in (3.4), do we have

$$\left\lfloor\frac{n-1}{4}\right\rfloor_n ! \equiv 1 \pmod n. \tag{3.5}$$

Although the left-hand side of (3.5) makes sense for all positive integers n, in order to avoid too many distinct cases, we consciously restrict our attention to odd n only. We begin with a negative result.

THEOREM 5. *With n as in (3.4), the Gauss factorial $\left\lfloor\frac{n-1}{4}\right\rfloor_n!$ cannot have*

(a) *orders* 1, 2, *or* 4 *when* $r = 1$, *with the exception of* $n = 15$;
(b) *orders* 1 *or* 2 *when* $r = 2$;
(b) *order* 1 *when* $r = 3$.

The three parts of this result are best possible in the sense that there are easy counterexamples when in addition to $p \equiv 1 \pmod 4$ we also have $q_1 \equiv 1 \pmod 4$ in (3.4). This is illustrated by the following examples.

EXAMPLE 1. (a) $n = 5 \cdot 29$, $n = 13 \cdot 17$, and $n = 5 \cdot 13$ are the smallest relevant examples for which $\operatorname{ord}_n \left(\frac{n-1}{4}\right)_n! = 1$, 2, and 4, respectively.

(b) $n = 5 \cdot 29 \cdot 3^2$ and $n = 5 \cdot 13 \cdot 3^2$ are the smallest relevant examples for which $\operatorname{ord}_n \left(\frac{n-1}{4}\right)_n! = 1$ and 2, respectively.

(c) $n = 5 \cdot 13 \cdot 3 \cdot 7$ is the smallest relevant example for which $\operatorname{ord}_n \left(\frac{n-1}{4}\right)_n! = 1$.

Returning to the case where n has exactly one prime factor $p \equiv 1 \pmod 4$, we now state our first main result.

THEOREM 6. *Let n be as in (3.4), with $r \geqq 4$. Then (3.5) holds if and only if*

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

(iii) $r \geqq \ell$.

When $\ell = 4$, *the congruence* (3.5) *implies* $\alpha = 1$.

The last statement will be proved in Section 5 below, while the rest of this result is a direct consequence of the following Theorem 7. It will also be shown in Section 5 that a prime $p \equiv 1 \pmod 4$ for which Condition (i) holds, necessarily satisfies $\operatorname{ord}_p\left(\frac{p-1}{4}\right)! = 2^\ell$; that is, p is a Gauss prime of level ℓ.

Theorem 6 immediately explains the example from the end of Section 1:

EXAMPLE 2. Let $p := 46817$; as we saw, it is a Gauss prime of level 4, so (i) holds with $\ell = 4$. Next, we note that

$$p + 1 = 2 \cdot 3^4 \cdot 17^2, \qquad p - 1 = 2^5 \cdot 7 \cdot 11 \cdot 19.$$

Therefore, if we set $n = 46817 \cdot 3^{\beta_1} \cdot 7 \cdot 11 \cdot 19$, with $1 \leqq \beta_1 \leqq 4$, then conditions (ii) and (iii) are both satisfied, and we obtain four different integers n for which the congruence (3.5) holds. (We will consider larger examples later in this paper).

On the other hand, if p is one of the first three Gauss primes of level 4, namely 17, 241, or 3361, then there are fewer than four prime divisors q_j of $p+1$ or $p-1$ with $q_j \equiv -1 \pmod 4$. Similarly, each one of the other known Gauss primes of level $\ell \geqq 5$ (see Table 4) has fewer than ℓ such prime divisors q_j. This means that none of these primes will lead to solutions of (3.5).

In spite of this, there is still a great deal we can say about these Gauss primes. To motivate our next result, we consider the following example.

EXAMPLE 3. Consider $p := 262\,337$, a Gauss prime of level 5 (see Table 4). We have

$$p + 1 = 2 \cdot 3 \cdot 23 \cdot 1901, \qquad p - 1 = 2^6 \cdot 4099,$$

and the prime factors of interest are $q_1 = 3$, $q_2 = 23$ and $q_3 = 4099$. Then

$$\operatorname{ord}_n \left\lfloor \frac{n-1}{4} \right\rfloor_n ! = \begin{cases} 32 & \text{when } n = p, \\ 16 & \text{when } n = pq_i,\ 1 \leqq i \leqq 3, \\ 8 & \text{when } n = pq_iq_j,\ 1 \leqq i < j \leqq 3, \\ 4 & \text{when } n = pq_1q_2q_3. \end{cases}$$

Thus, multiplying n by a new prime factor q_j (of $p+1$ or $p-1$) lowers the order of $\left\lfloor \frac{n-1}{4} \right\rfloor_n !$ by a factor of 2 each time. This is in fact true in general, as the following theorem, our second main result, shows.

THEOREM 7. *Suppose the prime* $p \equiv 1 \pmod 4$ *and the integer* $\alpha \geqq 1$ *are such that*

$$\operatorname{ord}_{p^\alpha} \left(\frac{p^\alpha - 1}{4} \right)_p ! = 2^\ell \quad \textit{for some} \quad \ell \geqq 4. \tag{3.6}$$

If n *is an integer of the form* (3.4) *such that*

$$q_j^{\beta_j} \mid p-1 \quad \textit{or} \quad q_j^{\beta_j} \mid p+1 \quad \textit{for} \quad j = 1, \dots, r, \tag{3.7}$$

then

$$\operatorname{ord}_n \left\lfloor \frac{n-1}{4} \right\rfloor_n ! = \begin{cases} 2^{\ell - r} & \textit{when } r \leqq \ell, \\ 1 & \textit{when } r > \ell. \end{cases} \tag{3.8}$$

It is clear that this result immediately implies all but the last statement of Theorem 6. Theorem 7, in turn, will be proved in Section 5, as a consequence of certain closed-form congruences which will be obtained in the next section.

4. Some key lemmas

The proofs of Theorems 5–8 depend in an essential way on certain closed-form congruences which will be stated and proved in this section. In order to obtain congruences such as (3.5), we use the Chinese Remainder Theorem, combining the moduli p^α and w. Thus, given a positive integer n as in (3.4), we are going to derive congruences for $\left\lfloor \frac{n-1}{4} \right\rfloor_n !$, separately modulo p^α and w, and for the first congruence also separately for $n \equiv \pm 1 \pmod 4$.

LEMMA 2. *Let* $n \equiv 1 \pmod 4$ *be as in* (3.4). *Then*

$$\left(\frac{n-1}{4} \right)_n ! \equiv A_r(n) \left(\frac{p^\alpha - 1}{4} \right)_p !^{2^r} \pmod{p^\alpha}, \tag{4.1}$$

where

$$A_r(n) = \begin{cases} (-1)^{\frac{p+q_1}{4}} q_1^{\frac{1}{4}\varphi(p^\alpha)}, & r = 1, \\ (q_1 q_2)^{\frac{1}{2}\varphi(p^\alpha)}, & r = 2, \\ 1, & r \geqq 3. \end{cases} \tag{4.2}$$

We mention at this point that in contrast to similar closed forms obtained in [5], where n has two prime factors congruent to 1 modulo 4, the congruence (4.1) does not depend on any of the powers β_j; in fact, for $r \geqq 3$, there is no dependence on the primes q_j at all.

PROOF OF LEMMA 2. With the aim of splitting the Gauss factorial $\left(\frac{n-1}{4}\right)_n!$ into convenient smaller products, we write

$$\frac{n-1}{4} = \frac{p^\alpha w - 1}{4} = \frac{w-1}{4}p^\alpha + \frac{p^\alpha - 1}{4}.$$

Based on this, we write

$$\left(\frac{n-1}{4}\right)_n! = \left(\prod_{j=1}^{\frac{w-1}{4}} P_j\right) Q, \tag{4.3}$$

where

$$P_j := \prod_{\substack{k=1 \\ \gcd\left((j-1)p^\alpha+k,n\right)=1}}^{p^\alpha-1} \left((j-1)p^\alpha + k\right),$$

$$Q := \prod_{\substack{k=1 \\ \gcd\left((w-1)p^\alpha/4+k,n\right)=1}}^{\frac{p^\alpha-1}{4}} \left(\frac{w-1}{4}p^\alpha + k\right).$$

Now define

$$\overline{P_j} := \prod_{\substack{k=1 \\ \gcd\left((j-1)p^\alpha+k,p\right)=1}}^{p^\alpha-1} \left((j-1)p^\alpha + k\right),$$

$$\overline{Q} := \prod_{\substack{k=1 \\ \gcd\left((w-1)p^\alpha/4+k,p\right)=1}}^{\frac{p^\alpha-1}{4}} \left(\frac{w-1}{4}p^\alpha + k\right),$$

so the products $\overline{P_j}$ and $\overline{Q}$ include multiples of 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

$$\overline{P_j} \equiv \prod_{\substack{k=1 \\ \gcd(k,p)=1}}^{p^\alpha-1} k = (p^\alpha - 1)_p! \equiv -1 \pmod{p^\alpha} \tag{4.4}$$

by the Gauss–Wilson theorem (1.2), and

$$\overline{Q} \equiv \prod_{\substack{k=1 \\ \gcd(k,p)=1}}^{\frac{p^\alpha-1}{4}} k = \left(\frac{p^\alpha-1}{4}\right)_p ! \pmod{p^\alpha}. \tag{4.5}$$

The quantity

$$\left(\prod_{j=1}^{\frac{w-1}{4}} \overline{P_j}\right)\overline{Q} \tag{4.6}$$

is the product of all integers from 1 to $\frac{n-1}{4}$, without multiples of p. To reduce this product to $\left(\frac{n-1}{4}\right)_n !$ in (4.3), we use the inclusion/exclusion principle and first divide the product (4.6) by all the multiples of $q_1, \dots, q_r$, then multiply it by all the multiples (if any) of $q_{j_1}q_{j_2}$, $1 \leqq j_1 < j_2 \leqq r$, then divide by all the multiples (if any) of $q_{j_1}q_{j_2}q_{j_3}$, $1 \leqq j_1 < j_2 < j_3 \leqq r$, etc. To do this, we define for a given k, $1 \leqq k \leqq r$ and $1 \leqq j_1 < \dots < j_k \leqq r$, the product

$$\Pi(j_1, \dots, j_k) = \prod_{\substack{\nu=1 \\ \gcd(\nu,p)=1}}^{m(j_1,\dots,j_k)} (\nu q_{j_1} \dots q_{j_k}), \tag{4.7}$$

where

$$m(j_1, \dots, j_k) = \left\lfloor \frac{(n-1)/4}{q_{j_1} \dots q_{j_k}} \right\rfloor = \frac{1}{4}\left(\frac{p^\alpha q_1^{\beta_1} \cdots q_r^{\beta_r}}{q_{j_1} \dots q_{j_k}} - 2 + (-1)^k\right).$$

Now for even $k \geqq 2$ we get

$$\begin{aligned} m(j_1, \dots, j_k) &= \frac{1}{4}\left(\frac{q_1^{\beta_1} \cdots q_r^{\beta_r}}{q_{j_1} \dots q_{j_k}} - 1\right)p^\alpha + \frac{p^\alpha-1}{4} \\ &= M(j_1, \dots, j_k)p^\alpha + \frac{p^\alpha-1}{4}, \end{aligned} \tag{4.8}$$

and for odd $k \geqq 1$,

$$\begin{aligned} m(j_1, \dots, j_k) &= \frac{1}{4}\left(\frac{q_1^{\beta_1} \cdots q_r^{\beta_r}}{q_{j_1} \dots q_{j_k}} - 3\right)p^\alpha + \frac{3(p^\alpha-1)}{4} \\ &= M(j_1, \dots, j_k)p^\alpha + \frac{3(p^\alpha-1)}{4}. \end{aligned} \tag{4.9}$$

With (4.7) and (4.8) we therefore have for even $k \geqq 2$,

$$\Pi(j_1,\dots,j_k) \equiv \left[(q_{j_1}\dots q_{j_k})^{\varphi(p^\alpha)}(p^\alpha-1)_p!\right]^{M(j_1,\dots,j_k)} \times (q_{j_1}\dots q_{j_k})^{\varphi(p^\alpha)/4}\left(\frac{p^\alpha-1}{4}\right)_p! \pmod{p^\alpha}$$

$$\equiv (-1)^{M(j_1,\dots,j_k)}(q_{j_1}\dots q_{j_k})^{\varphi(p^\alpha)/4}\left(\frac{p^\alpha-1}{4}\right)_p! \pmod{p^\alpha}, \tag{4.10}$$

by Euler's generalization of Fermat's little theorem and by the Gauss–Wilson theorem. Similarly, (4.7) and (4.9) give for odd $k \geqq 1$,

$$\Pi(j_1,\dots,j_k) \equiv \left[(q_{j_1}\dots q_{j_k})^{\varphi(p^\alpha)}(p^\alpha-1)_p!\right]^{M(j_1,\dots,j_k)} \times (q_{j_1}\dots q_{j_k})^{3\varphi(p^\alpha)/4}\left(\frac{3(p^\alpha-1)}{4}\right)_p! \pmod{p^\alpha}$$

$$\equiv (-1)^{M(j_1,\dots,j_k)}(q_{j_1}\dots q_{j_k})^{3\varphi(p^\alpha)/4}\left(\frac{3(p^\alpha-1)}{4}\right)_p! \pmod{p^\alpha}. \tag{4.11}$$

Now, comparing (4.3) with (4.6) and using inclusion/exclusion as discussed following (4.6), we get

$$\left(\frac{n-1}{4}\right)_n! = \left(\prod_{j=1}^{\frac{w-1}{4}}\overline{P_j}\right)\overline{Q}\prod_{k=1}^{r}\prod_{1\leqq j_1<\dots<j_k\leqq r}\left(\Pi(j_1,\dots,j_k)\right)^{(-1)^k}$$

$$\equiv (-1)^{\frac{w-1}{4}}\left(\frac{p^\alpha-1}{4}\right)_p!\prod_{k=1}^{r}\prod_{1\leqq j_1<\dots<j_k\leqq r}\left(\Pi(j_1,\dots,j_k)\right)^{(-1)^k} \pmod{p^\alpha} \tag{4.12}$$

where we have used (4.4) and (4.5). The right-most term in (4.12) shows that for even $k \geqq 2$ the right-hand side of (4.10) is in the numerator, while for odd $k \geqq 1$ the right-hand side of (4.11) is in the denominator. With this in mind, we consider the product

$$\left(\frac{3(p^\alpha-1)}{4}\right)_p!(-1)^{\frac{p-1}{4}}\left(\frac{p^\alpha-1}{4}\right)_p! \equiv (p^\alpha-1)_p! \equiv -1 \pmod{p^\alpha},$$

where the second congruence follows from the Gauss–Wilson theorem. Hence

$$\left(\left(\frac{3(p^\alpha-1)}{4}\right)_p!\right)^{-1} \equiv (-1)^{\frac{p+3}{4}}\left(\frac{p^\alpha-1}{4}\right)_p! \pmod{p^\alpha}. \tag{4.13}$$

To continue with the proof of Lemma 2, we first consider the case $r = 1$. In this case the right-hand side of (4.12), together with (4.11) and (4.13), reduces to

(4.14)
$$\left(\frac{n-1}{4}\right)_n ! \equiv (-1)^{\frac{w-1}{4}+M(j_1)+\frac{p+3}{4}} \left(\frac{p^\alpha-1}{4}\right)_p !^2 q_1^{-3\varphi(p^\alpha)/4} \pmod{p^\alpha}.$$

Since $q_1 \equiv 3 \pmod 8$ or $\equiv 7 \pmod 8$ and β_1 is even (recall that $n \equiv 1 \pmod 4$ and thus $w = q_1^{\beta_1} \equiv 1 \pmod 4$), we have in fact $q_1^{\beta_1} \equiv 1 \pmod 8$ and $q_1^{\beta_1-1} \equiv q_1 \pmod 8$. Therefore

$$\frac{w-1}{4} = \frac{1}{4}\big(q_1^{\beta_1}-1\big) \equiv 0 \pmod 2,$$

$$M(j_1) = \frac{1}{4}\big(q_1^{\beta_1-1}-3\big) \equiv \frac{1}{4}(q_1-3) \pmod 2,$$

so that the exponent of (-1) in (4.14) reduces to $\frac{1}{4}(p+q_1)$. Next, by Euler's generalization of Fermat's little theorem we have

$$q_1^{-3\varphi(p^\alpha)/4} \equiv q_1^{\varphi(p^\alpha)/4} \pmod{p^\alpha},$$

and this, with (4.14), finally gives the congruence (4.1) with the first part of (4.2).

For the remainder of the proof we may therefore assume that $r \geqq 2$. We use again (4.12) and deal separately with the three factors in each of the right-hand sides of (4.10) and (4.11). In two of the three cases we need the combinatorial fact that the number of products $\Pi(j_1,\dots,j_k)$, $1 \leqq k \leqq r$ and $r \geqq 2$ in (4.12) for k even and odd is respectively

$$\sum_{k=1}^{r} \sum_{\substack{1\leqq j_1<\dots<j_k\leqq r \\ k \text{ even}}} 1 = \sum_{j=1}^{\lfloor \frac{r}{2} \rfloor} \binom{r}{2j} = 2^{r-1}-1, \tag{4.15}$$

$$\sum_{k=1}^{r} \sum_{\substack{1\leqq j_1<\dots<j_k\leqq r \\ k \text{ odd}}} 1 = \sum_{j=0}^{\lfloor \frac{r-1}{2} \rfloor} \binom{r}{2j+1} = 2^{r-1}. \tag{4.16}$$

The evaluations of the binomial sums above are well-known and can be found, e.g., in [10], identities (1.97) and (1.89).

We begin with the powers of (-1) in (4.10) and (4.11). Since the exponent $(-1)^k$ in (4.12) does not make any difference, the contributions from $(-1)^{M(j_1,\dots,j_k)}$ will be $(-1)^A$, where by (4.8) and (4.9) we have

$$A = \sum_{k=1}^{r} \sum_{\substack{1\leqq j_1<\cdots<j_k\leqq r\\ k \text{ even}}} M(j_1,\dots,j_k) + \frac{w-1}{4}$$

$$= \frac{q_1^{\beta_1}\cdots q_r^{\beta_r}}{4} \sum_{k=0}^{r} \sum_{\substack{1\leqq j_1<\cdots<j_k\leqq r\\ k \text{ even}}} \frac{1}{q_{j_1}\dots q_{j_k}} - \frac{1}{4}2^{r-1} - \frac{3}{4}2^{r-1},$$

where we have used (4.15) and (4.16) in the second equation. The last double sum can be written as a product, and we obtain

$$A = \frac{q_1^{\beta_1}\cdots q_r^{\beta_r}}{4} \prod_{j=1}^{r} \frac{q_j+1}{q_j} - 2^{r-1} = \frac{1}{4}\prod_{j=1}^{r} q_j^{\beta_j-1}(q_j+1) - 2^{r-1} \equiv 0 \pmod 2,$$

where the final congruence holds for $r \geqq 2$, which is clear if we recall that $q_j \equiv -1 \pmod 4$ for all $1 \leqq j \leqq r$. This shows that for $r \geqq 2$ the term $A_r(n)$ in (4.2) is positive.

Next we deal with the powers of $q_{j_1}\dots q_{j_k}$ in (4.10) and (4.11). We fix a j, $1 \leqq j \leqq r$, and observe that for a given k, $1 \leqq k \leqq r$, the prime q_j to its appropriate power occurs $\binom{r-1}{k-1}$ times (since j is fixed and the remaining $k-1$ subscripts vary). So in total, when k is even (respectively odd), q_j to its appropriate power occurs in (4.12)

$$\sum_{j=0}^{\lfloor\frac{r-2}{2}\rfloor} \binom{r-1}{2j+1} = 2^{r-2} \text{ times } (k \text{ even}),$$

$$\sum_{j=0}^{\lfloor\frac{r-1}{2}\rfloor} \binom{r-1}{2j} = 2^{r-2} \text{ times } (k \text{ odd}).$$

This means that altogether we have for each j, $1 \leqq j \leqq r$,

$$q_j^{2^{r-2}\varphi(p^\alpha)/4} \qquad \text{and} \qquad q_j^{2^{r-2}3\varphi(p^\alpha)/4}$$

in the numerator, respectively the denominator of (4.12). The exact power of q_j in (4.12) is then

$$q_j^{-2^{r-3}\varphi(p^\alpha)} \equiv \begin{cases} q_j^{\frac{1}{2}\varphi(p^\alpha)} \pmod{p^\alpha} & \text{when } r = 2, \\ 1 \pmod{p^\alpha} & \text{when } r \geqq 3, \end{cases}$$

where the congruences follow from Euler's generalization of Fermat's little theorem. This leads to the second and third parts in (4.2).

Finally, we consider the right-most factors in (4.10) and (4.11), namely the respective Gauss factorials. The number of times each of the two occurs is given by (4.15) and (4.16). Using (4.13), we find that the total contribution of these terms to (4.12), including the one factor $\left(\frac{p^\alpha-1}{4}\right)_p!$ in (4.12), is

$$\left(\frac{\left(\frac{p^\alpha-1}{4}\right)_p!}{\left(\frac{3(p^\alpha-1)}{4}\right)_p!}\right)^{2^{r-1}} \equiv (-1)^{\frac{p+3}{4}2^{r-1}} \left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^{2^r} \pmod{p^\alpha}.$$

Now, for $r \geqq 2$ the sign on the right is positive. This gives the congruence (4.1), thus completing the proof of Lemma 2. □

The following lemma complements Lemma 2. The proof is very similar to that of Lemma 2, and we omit the details.

LEMMA 3. *Let $n \equiv -1 \pmod 4$ be as in (3.4). Then*

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n ! \equiv A_r(n)^{-1} \left(\frac{p^\alpha-1}{4}\right)_p !^{-2^r} \pmod{p^\alpha}, \tag{4.17}$$

where $A_r(n)$ is as defined in (4.2).

The congruences (4.1) and (4.17) could be combined into one, but for greater clarity we have stated them as separate lemmas.

For the next lemma we need the following definitions, taken from D. H. Lehmer's paper [11]. For positive integers $k < n$ we define, for each $q = 0, 1, \ldots, k-1$, the partial totient function $\varphi(k, q, n)$ as the number of totatives τ, that is, integers τ relatively prime to n, for which

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

Here we will be dealing with the special case

$$\varphi(4, 1, w) = \#\left\{\tau \,\middle|\, 1 \leqq \tau \leqq \frac{w-1}{4},\ \gcd(\tau, w) = 1\right\}. \tag{4.18}$$

We are now ready to state and prove

LEMMA 4. *Let n be as in (3.4). Then*

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n ! \equiv \frac{B_r(n)}{p^{\varphi(4,1,w)}} \pmod{w}, \tag{4.19}$$

where

$$B_r(n) = \begin{cases} (-1)^{(p-1)/4}, & r = 1, \\ 1, & r \geqq 2. \end{cases} \tag{4.20}$$

Again we mention at this point that while the Gauss factorial on the left-hand side of (4.19) has α-dependencies, the right-hand side has none.

PROOF OF LEMMA 4. We first assume that $n \equiv 1 \pmod 4$, which also means, by (3.4), that $w \equiv 1 \pmod 4$. Proceeding in a similar way as in the proof of Lemma 2, we divide $\frac{n-1}{4}$ by w with remainder and obtain

$$\frac{n-1}{4} = \frac{p^\alpha w - 1}{4} = mw + \frac{w-1}{4},$$

where $m := (p^\alpha - 1)/4$. Based on this, we write

$$\left(\frac{n-1}{4}\right)_n ! = \left(\prod_{j=1}^{m} P_j\right) Q, \tag{4.21}$$

where this time we have, for all $j = 1, \ldots, m$,

$$P_j := \prod_{\substack{k=1 \\ \gcd\left((j-1)w+k,n\right)=1}}^{w} \left((j-1)w+k\right), \qquad Q := \prod_{\substack{k=1 \\ \gcd\left(mw+k,n\right)=1}}^{\frac{w-1}{4}} (mw+k).$$

As in the proof of Lemma 2 we now define the corresponding 'augmented' products

$$\overline{P_j} := \prod_{\substack{k=1 \\ \gcd\left((j-1)w+k,w\right)=1}}^{w} \left((j-1)w+k\right), \qquad \overline{Q} := \prod_{\substack{k=1 \\ \gcd\left(mw+k,w\right)=1}}^{\frac{w-1}{4}} (mw+k),$$

so the products $\overline{P_j}$ and $\overline{Q}$ include multiples of p that are relatively prime to w. Before taking this into account in evaluating (4.21), we note that by

the Gauss–Wilson theorem we have for $1 \leqq j \leqq m$,

$$\overline{P_j} \equiv \prod_{\substack{k=1 \\ \gcd(k,w)=1}}^{w} k = (w-1)_w! \equiv \begin{cases} -1 \pmod{w} & \text{if } r = 1, \\ 1 \pmod{w} & \text{if } r \geqq 2, \end{cases} \tag{4.22}$$

$$\overline{Q} \equiv \prod_{\substack{k=1 \\ \gcd(k,w)=1}}^{\frac{w-1}{4}} k = \left(\frac{w-1}{4}\right)_w! \pmod{w}. \tag{4.23}$$

Now the product $\overline{P_1} \cdots \overline{P_m} \cdot \overline{Q}$ can be reduced to the product (4.21) by dividing the former by

$$\Pi_1 := \prod_{\substack{\nu=1 \\ \gcd(\nu,w)=1}}^{m_1} (\nu p), \tag{4.24}$$

where

$$m_1 = \left\lfloor \frac{(n-1)/4}{p} \right\rfloor = \frac{p^{\alpha-1}w - 1}{4}, \tag{4.25}$$

where the second equality follows from the obvious division

$$\frac{n-1}{4} = m_1 p + \frac{p-1}{4}.$$

To evaluate Π_1 modulo w, we divide once again with remainder:

$$m_1 = M_1 w + \frac{w-1}{4}, \qquad \text{where} \qquad M_1 := \frac{p^{\alpha-1}-1}{4}; \tag{4.26}$$

note that by assumption all quotients are integers. With (4.24) and (4.26) we get

$$\Pi_1 \equiv \left(p^{\varphi(w)}(w-1)_w!\right)^{M_1} p^{\varphi(4,1,w)} \left(\frac{w-1}{4}\right)_w! \pmod{w} \tag{4.27}$$

$$\equiv (-1)^{s(r)M_1} p^{\varphi(4,1,w)} \left(\frac{w-1}{4}\right)_w! \pmod{w},$$

where $s(r) = 1$ when $r = 1$ and $s(r) = 0$ when $r > 1$, having used the Euler–Fermat theorem and the Gauss–Wilson theorem. With (4.21)–(4.23) and (4.27) we now obtain

$$\left(\frac{n-1}{4}\right)_n ! \equiv \frac{\overline{P_1}\cdots\overline{P_m}\cdot\overline{Q}}{\Pi_1} \equiv \frac{(-1)^{s(r)(m-M_1)}}{p^{\varphi(4,1,w)}} \pmod{w}. \tag{4.28}$$

Finally we note that

$$m - M_1 = \frac{p^\alpha - 1}{4} - \frac{p^{\alpha-1}-1}{4} = \frac{p^{\alpha-1}(p-1)}{4} \equiv \frac{p-1}{4} \pmod 2,$$

and this, with (4.28), gives (4.19) and (4.20) for $n \equiv 1 \pmod 4$. The case $n \equiv 3 \pmod 4$ is very similar and requires only minor adjustments in the various divisions with remainder. □

5. Proofs of Theorems 5–7

We are now ready to prove our main results, Theorems 6 and 7, along with the supplementary Theorem 5, using the closed-form congruences obtained in the previous section. We first need another lemma concerning the counting function $\varphi(4,1,w)$ introduced in (4.18).

LEMMA 5. *With w as in (3.4), we have*

$$4\varphi(4,1,w) = \varphi(w) \pm 2^r, \tag{5.1}$$

with "$\pm$" corresponding to $w \equiv \pm 1 \pmod 4$. In particular, $2^{r-2} \mid \varphi(4,1,w)$ for $r \geqq 2$.

PROOF. (5.1) is a direct consequence of Theorem 3 in [11, p. 351]. The second statement then follows from the fact that $\varphi(w)$ is divisible by 2^r since w is the product of powers of r distinct odd primes. □

PROOF OF THEOREM 7. (1) We begin with $r = 1$, i.e., $n = p^\alpha q_1^{\beta_1}$, with q_1 satisfying (3.7). By (4.1), (4.2), and (4.17) we have

$$\left\lfloor\frac{n-1}{4}\right\rfloor_n ! \equiv \left((-1)^{\frac{p+q_1}{4}} q_1^{\frac{1}{4}\varphi(p^\alpha)} \left(\frac{p^\alpha-1}{4}\right)_p !^2\right)^{\pm 1} \pmod{p^\alpha}, \tag{5.2}$$

and by (4.19), (4.20),

$$\left\lfloor\frac{n-1}{4}\right\rfloor_n ! \equiv \frac{(-1)^{(p-1)/4}}{p^{\varphi(4,1,w)}} \pmod{w}. \tag{5.3}$$

We first note that

$$\left((-1)^{\frac{p+q_1}{4}}\right)^{2^{\ell-2}} = (-1)^{(p+q_1)2^{\ell-4}} = 1$$

since $2^{\ell-4}$ is an integer and $p+q_1$ is even. Furthermore,

$$\left(q_1^{\frac{1}{4}\varphi(p^\alpha)}\right)^{2^{\ell-2}} = \left(q_1^{2^{\ell-4}}\right)^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha},$$

by Euler's generalization of Fermat's Little Theorem. Hence (5.2) gives

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n !^{2^{\ell-2}} \equiv \left(\frac{p^\alpha - 1}{4} \right)_p !^{\pm 2^{\ell-1}} \equiv -1 \pmod{p^\alpha}, \tag{5.4}$$

where the second congruence follows from (3.6). Next we have

$$\left((-1)^{(p-1)/4}\right)^{2^{\ell-1}} = (-1)^{(p-1)2^{\ell-3}} = 1.$$

Furthermore, (3.7) implies $p \equiv \pm 1 \pmod{w}$, where we note that $w = q_1^{\beta_1}$, and thus

$$\left(p^{\varphi(4,1,w)}\right)^{2^{\ell-1}} \equiv (\pm 1)^{\varphi(4,1,w)2^{\ell-1}} = 1 \pmod{w}, \tag{5.5}$$

so that with (5.3) we get

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n !^{2^{\ell-1}} \equiv 1 \pmod{w}.$$

This, with (5.4) and the Chinese Remainder Theorem, gives

$$\operatorname{ord}_n \left\lfloor \frac{n-1}{4} \right\rfloor_n ! = 2^{\ell-1}. \tag{5.6}$$

(2) Next, let $r = 2$, i.e., $n = p^\alpha q_1^{\beta_1} q_2^{\beta_2}$, with q_1, q_2 satisfying (3.7). Again by (4.1), (4.2), and (4.17) we have

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n ! \equiv \left((q_1 q_2)^{\frac{1}{2}\varphi(p^\alpha)} \left(\frac{p^\alpha - 1}{4} \right)_p !^4 \right)^{\pm 1} \pmod{p^\alpha}, \tag{5.7}$$

and by (4.19), (4.20),

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n ! \equiv \frac{1}{p^{\varphi(4,1,w)}} \pmod{w}. \tag{5.8}$$

Similarly to the first part we note that

$$\left((q_1q_2)^{\frac{1}{2}\varphi(p^\alpha)}\right)^{2^{\ell-3}} = \left((q_1q_2)^{2^{\ell-4}}\right)^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha},$$

and (5.7) gives

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n !^{2^{\ell-3}} \equiv \left(\frac{p^\alpha - 1}{4}\right)_p !^{\pm 2^{\ell-1}} \equiv -1 \pmod{p^\alpha}. \tag{5.9}$$

Just as in (5.5) we also get

$$\left(p^{\varphi(4,1,w)}\right)^{2^{\ell-2}} \equiv (\pm 1)^{\varphi(4,1,w)2^{\ell-2}} = 1 \pmod{q_j^{\beta_j}} \tag{5.10}$$

for $j = 1, 2$. By the Chinese Remainder Theorem, (5.10) then holds for $w = q_1^{\beta_1}q_2^{\beta_2}$ as well, and with (4.19) we get

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n !^{2^{\ell-2}} \equiv 1 \pmod{w}.$$

This, with (5.9) and using the Chinese Remainder Theorem again, gives

$$\operatorname{ord}_n \left\lfloor \frac{n-1}{4} \right\rfloor_n ! = 2^{\ell-2}. \tag{5.11}$$

(3) Now let $3 \leqq r < \ell$. Then once again (4.1), (4.2), and (4.17) give

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n !^{2^{\ell-r-1}} \equiv \left(\left(\frac{p^\alpha - 1}{4}\right)_p !^{2^r}\right)^{\pm 2^{\ell-r-1}} \tag{5.12}$$

$$\equiv \left(\frac{p^\alpha - 1}{4}\right)_p !^{\pm 2^{\ell-1}} \equiv -1 \pmod{p^\alpha}.$$

Furthermore, in analogy to (5.10) we have, since $\ell > r$,

$$\left(p^{\varphi(4,1,w)}\right)^{2^{\ell-r}} \equiv (\pm 1)^{\varphi(4,1,w)2^{\ell-r}} = 1 \pmod{q_j^{\beta_j}} \tag{5.13}$$

for all $j = 1, 2, \ldots r$, and so (5.13) also holds modulo w. With (4.19) we then get

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n !^{2^{\ell-r}} \equiv 1 \pmod{w}. \tag{5.14}$$

As before, the Chinese Remainder Theorem applied to (5.12) and (5.14) gives

$$\operatorname{ord}_n \left\lfloor \frac{n-1}{4} \right\rfloor_n ! = 2^{\ell-r} \quad (\ell > r). \tag{5.15}$$

(4) Finally, let $r \geqq \ell \geqq 4$. Then by (4.1), (4.2), and (4.17), together with (3.6), we have

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n !^{2^{\ell-r}} \equiv 1 \pmod{p^\alpha}. \tag{5.16}$$

Next, since $r \geqq 4$, Lemma 5 shows that $\varphi(4,1,w) = 2^{r-3}E$, where E is an even integer. Hence

$$\varphi(4,1,w)2^{\ell-r} = 2^{\ell-3}E,$$

which is even, so that (5.13) holds also in the case $r \geqq \ell \geqq 4$, and thus (5.14) holds as well. This, together with (5.16), gives

$$\operatorname{ord}_n \left\lfloor \frac{n-1}{4} \right\rfloor_n ! = 1 \quad (r \geqq \ell \geqq 4). \tag{5.17}$$

Altogether, (5.6), (5.11), (5.15) and (5.17) combined give (3.8), which completes the proof of Theorem 7. □

Proof of Theorem 5. We raise both sides of (5.2) and (5.3) to the 4th power, assuming that the order in question is 1, 2, or 4. Then the left-hand sides are 1 modulo p^α and modulo $w = q_1^{\beta_1}$, respectively. From (5.2) we get

$$\left(\frac{p^\alpha - 1}{4} \right)_p !^8 \equiv 1 \pmod{p^\alpha}, \tag{5.18}$$

and by Corollary 3 this holds only when $\alpha = 1$ and $p = 5$. From (5.3) and Lemma 5 we get

$$1 = p^{4\varphi(4,1,w)} = 5^{\varphi(w)\pm 2},$$

which forces the exponent to be 0 and thus $w = q_1^{\beta_1} = 3 (\equiv -1 \pmod 4)$. Hence $n = pw = 15$ is the only possible solution; in fact, $\left\lfloor \frac{15-1}{4} \right\rfloor_{15} ! = 3_{15}!$ $= 1 \cdot 2 \equiv 2 \pmod{15}$, and clearly $\operatorname{ord}_{15} 2 = 4$.

(b) Assuming the the order in question is 1 or 2, we square both sides of (5.8). Once again the left-hand side becomes 1 modulo $w = q_1^{\beta_1} q_2^{\beta_2}$, respectively. With Lemma 5 we get

$$1 = p^{2\varphi(4,1,w)} = 5^{\frac{1}{2}\varphi(w)\pm 2}, \tag{5.19}$$

which again forces the exponent to be 0. However, since $r = 2$, we have $\varphi(w) \geqq \varphi(3 \cdot 7) = 12$, and (5.19) is impossible.

(c) Finally we assume that $r = 3$ and that the Gauss factorial in question is 1 modulo n. Then (4.19) and Lemma 5 give a condition similar to (5.19), which can again be shown to be impossible. This completes the proof of Theorem 5. □

As mentioned in Section 3, Theorem 7 implies all but the last statement of Theorem 6. For the proof of that statement we require a lemma which is of independent interest.

LEMMA 6. *Let $p \equiv 1 \pmod 4$ be a prime and $\alpha \geqq 2$. If*

$$\operatorname{ord}_{p^\alpha} \left(\frac{p^\alpha - 1}{4}\right)_p ! = 2^\ell \quad \textit{for some} \quad \ell \geqq 4, \tag{5.20}$$

then $\operatorname{ord}_p \left(\frac{p-1}{4}\right)! = 2^\ell$, i.e., p is a Gauss prime of level ℓ.

PROOF. Our main tool is the congruence (see Proposition 2.1 in [4])

$$\left(\frac{p^\alpha - 1}{4}\right)_p ! \equiv (-1)^{\frac{p-1}{4}} \left(\frac{p^{\alpha-1} - 1}{4}\right)_p ! \left(1 + c_\alpha(p) p^{\alpha-1}\right) \pmod{p^\alpha}, \tag{5.21}$$

where $c_\alpha(p)$ is an integer, and $\alpha \geqq 2$. Now the identity (5.20) is equivalent to

$$\left(\frac{p^\alpha - 1}{4}\right)_p !^{2^{\ell-1}} \equiv -1 \pmod{p^\alpha}. \tag{5.22}$$

Raising both sides of (5.21) to the power $2^{\ell-1}$ and taking the resulting congruences modulo $p^{\alpha-1}$, we get

$$\left(\frac{p^\alpha - 1}{4}\right)_p !^{2^{\ell-1}} \equiv \left(\frac{p^{\alpha-1} - 1}{4}\right)_p !^{2^{\ell-1}} \pmod{p^{\alpha-1}}.$$

Iterating this with α replaced by $\alpha - 1, \alpha - 2, \ldots, 2$, we obtain from (5.22) the corresponding congruence for $\alpha = 1$, as desired. □

We are now ready to prove the final statement of Theorem 6. By Lemma 6, any prime p that satisfies (i) for $\ell = 4$ is a Gauss prime of level 4. We are now going to show that for such primes we always have $\gamma_{\alpha+1} = p\gamma_\alpha$ (see (3.1) and (3.3)), i.e., the second alternative in Theorem 4 cannot occur.

In the forthcoming paper [6] we have shown that for arbitrary primes $p \equiv 1 \pmod 4$ the second alternative in Theorem 4 occurs if and only if

$$\left(2a - \frac{p}{2a}\right)^{p-1} \equiv 1 \pmod{p^2}, \tag{5.23}$$

where a is as in Theorem 1. We first expand

$$\left(2a - \frac{p}{2a}\right)^4 \equiv 16a^4 - 16a^2p = 16a^2(a^2 - p) = -16a^2b^2 \pmod{p^2},$$

where we have used the fact $p = a^2 + b^2$. Now by Theorem 3, p is a Gauss prime of level 4 if and only if $p - 1 = 4ab$. Hence, using the fact that $p \equiv 1 \pmod{16}$ by (2.9), we have

$$\left(2a - \frac{p}{2a}\right)^{p-1} \equiv (1-p)^{\frac{p-1}{2}} \equiv 1 - \frac{p-1}{2}p \equiv \frac{2+p}{2} \not\equiv 1 \pmod{p^2}.$$

This, with the condition (5.23), means that the identity (5.20) is in fact not possible for $\ell = 4$. This proves the final statement of Theorem 6.

Remark. We conjecture that this last statement of Theorem 6 holds for all $\ell \geqq 4$. However, the above proof relies in an essential way on Theorem 3, which does not seem to have an analogue for $\ell \geqq 5$.

6. Computations related to Gauss primes of level 4

As we saw in Section 2, Corollary 1 gives a characterization of all candidates for Gauss primes of level 4, and this makes it possible to find very large ones. In order to apply our main results, Theorems 6 and 7, we need to find prime factors congruent to 3 (mod 4) of $p - 1$ and/or $p + 1$. Fortunately, the necessary factorizations are greatly aided by the structure of the numbers p_k already explored around Corollary 1. The principal object in this connection is the sequence $\{a_k\}$ introduced in (2.9). First, comparing Theorem 3 and Corollary 1, we get

$$p_k = 4a_{k+1}a_k + 1 = a_{k+1}^2 + a_k^2, \tag{6.1}$$

which gives $2a_{k+1}a_k + 1 = a_{k+1}^2 - 2a_{k+1}a_k + a_k^2 = (a_{k+1} - a_k)^2$, and thus

$$p_k + 1 = 2(a_{k+1} - a_k)^2. \tag{6.2}$$

Second, to deal with the factors of $p_k - 1$, we use the fact that $a_k = U_k(4, 1)$ for $k \geqq 0$, and some of the known properties of the Lucas function, also known as generalized Lucas sequences (see, e.g., [17] or [18]), translate to

$$a_{2n+1} = (a_{n+1} - a_n)(a_{n+1} + a_n), \qquad a_{2n} = a_n(a_{n+1} - a_{n-1}). \tag{6.3}$$

Combining these identities with (6.1), and appropriately iterating the second identity, we get a partial factorization for each of the known Gauss primes p_k of level 4. Another important and very useful property of the generalized

Lucas sequences is the fact that they are divisibility sequences. This implies that

$$a_n \mid a_k \quad \text{whenever} \quad n \mid k. \tag{6.4}$$

The practical implications of the above are best illustrated by an example.

EXAMPLE 4. Consider p_{950}, the 12th Gauss prime of level 4. With (6.1) and repeated application of (6.3) we get

$$\begin{aligned} p_{950} - 1 &= 4a_{951}a_{950} \\ &= 4(a_{476} - a_{475})(a_{476} + a_{475})(a_{476} - a_{474}) \\ &\quad \times (a_{238} - a_{237})(a_{238} + a_{237}). \end{aligned} \tag{6.5}$$

Furthermore, since $950 + 1 = 3 \cdot 317$ and $949 + 1 = 2 \cdot 5^2 \cdot 19$, with (6.4) we see that $p_{950} - 1$ is also divisible by a_n for $n \in \{3, 317\} \cup \{2, 5, 10, 19, 25, 38, 50, 95, 190, 475\}$. Taking the gcd of these a_k with the factors in (6.5) will lead to further factors.

p	digits	support primes
p_1	2	$\mathbf{3}^2$
p_2	3	3, $\mathbf{11}^2$
p_3	4	3, 7
p_4	5	$\mathbf{3}^4$, 7, 11, 19
p_5	6	3, 11, 19, $\mathbf{571}^2$
p_{131}	150	3, 7, 23, 43, 263, 523, 571, $\mathbf{1051}^2$, 19387, 45795767 10177584143, 1242138477356291, 491822182778635763 $\mathbf{1403687828273374406026310517426017 9}^2$
p_{200}	229	3, 7, 11, 19, 79, 199, 499, 524899, 5961199, 17927599 66009919291, 46741076736673999, $\mathbf{4044362870707064404 3}^2$ 379357631304275170999, $\mathbf{q}_{73}^2$
p_{296}	339	3^3, 7, 23, 43, 571, $\mathbf{1187}^2$, 68204911, 15558008491 26947261171, $\mathbf{2692911311056409589 1}^2$ 513664040676430710837295376975820704523924 7
p_{350}	401	3^3, 11, 19, 71, 139, 499, 2131, 3691, 24851, 66499, 524899 33221392751, 2181060020651, 623497542978605645210351 $\mathbf{7799435399571419941722136 19}^2$
p_{519}	594	3, 7, 11, 19, 79, 103^2, 131, 347, 691, 1039, 2131, 2287, 2423 3691, 21107, 112111, 914131, 1067411, 1661659, 17927599 7584015919, 20048823079, 166135631419569172696867 9, $\mathbf{q}_{297}^2$

Table 5: The first ten Gauss primes of level 4; *complete list of support primes*

p	digits	support primes
p_{704}	806	3, 7, 11, 19, 23, 31, 43, 127, 571, 607, $\mathbf{2819}^2$, 16451, 20399 125311, 228799, 1154538818671039, 7897466719774591 320246565341022449819066263315559951668286536657 1, q_{166}
p_{950}	1087	3, 11, 19^2, 191, 379, 499, $\mathbf{3803}^2$, 4751, 110771, 524899, 909791 53304499, 2769867297143, 37970358201111142040047053951 q_{69}, q_{91}
p_{5598}	6404	3^2, 23, 43, 571, 1019, 15551, 48229787, 1114883439769991 46718088114419459, 9555057017674487443 $\mathbf{127978260359675772674659}^2$, 28935663175705018388294553 1 13165538109360189471454477326163823 9, q_{59}
p_{6683}	7645	3, 7, 83, 163^2, 26731, 13367, 68339443, 2302619203, 2610784387 202822125559, 348831164599, 98171768326967 367281209796743447, 8074835600027920615267 $\mathbf{2333263894292381557366 7}^2$, 10110807147744750514591999
p_{7445}	8517	3, 11, 19, 67, 443, 1459, 14891, 533063, 881987, 1962503 13650563, 192583051, 86373980496704851084067, q_{424} 69228718914562572367851791, 427771359361172203770659593 9
p_{8775}	10038	3^3, 7, 11, 19, 131, 499, 2131, 3691, 17551, 524899, 1661659 $\mathbf{23974667}^2$, 23308959463, 5354296361903, 9298768013263 741434566628911, 7420007032487139752228323 1746718602327738440396905 1, 463717788927030144456349419287 2390909755231165101933696689806 1899
p_{8786}	10051	3, 47, 59, 383, 53731, 64439, 138907099, 459396683, 1745648851 38986408754879, 69919681827766627, 8526373736976062503387 14323819521955732500251, $\mathbf{3919186241464072868392 27}^2$ 11908479788953299195698122686037 1
p_{11565}	13230	3^2, 11, 19, 23131, 16678171, $\mathbf{135362611}^2$, 10947438767 276588109571, 90052342255243, 232338985536060499 202533476147607459131, 2584661107817908726811 113951355040539709615756877854171, q_{271}
p_{12483}	14280	3^2, 7, 1459, 24967, 110771, 881987, 13650563, 192583051 47631288087127, 147240626734939, 222795845833051 2307861650648064971281111, 4894716277684700099236438894 03 3292365506603074396269587018851

Table 6: The next nine Gauss primes of level 4 *with all known support primes*

While the $p_k - 1$ have all these algebraic factors, in the case of $p_k + 1$, referring to (6.2) and noting that $a_{k+1} - a_k$ is itself prime for $k = 519$, we cannot expect any further algebraic factors for $p_k + 1$.

In practice, after all the above algebraic factors were identified (using Maple), we first checked them for probable primality and small prime factors, again using Maple, and in some cases PARI/GP. Following this, all remaining composite factors were subjected to a general-purpose factoring program due to Richard Crandall [7] which includes the Pollard rho, Pollard

$p-1$, and as its main component an implementation of the elliptic curve algorithm. Any remaining composite factors up to about 140 decimal digits were then factored using CADO-NFS [9], an implementation of the number field sieve. For the first ten Gauss primes of level 4, up to p_{519}, complete factorizations have been achieved. The resulting support prime powers are listed in Table 5, where the factors of p_k+1 are shown in bold. Very large prime factors are listed as q_d, where d is their number of decimal digits.

From p_{704} on, an increasing number of factors of p_k+1 and p_k-1 remain composite. For instance, $p_{704}+1$ has a 391-digit composite factor, while $p_{950}\pm 1$ have 489- and 183-digit composite factors, respectively, which have resisted all factorization attempts. Partial lists of support primes are given in Table 6. All three composites mentioned above are $\equiv 1 \pmod 4$, so it is possible that all their prime factors belong to the same residue class; therefore the lists for p_{704} and/or p_{950} may be complete after all. However, all further $p_k\pm 1$ have at least one composite factor $\equiv 3 \pmod 4$, and therefore the corresponding lists of support primes are definitely incomplete. As already mentioned following Table 3, we found five more p_k which are probable primes, having passed the `ispseudoprime` test of PARI/GP. These are $k = 13536$, 18006, 18995, 48773, and 93344. There are no others for $k \leqq 100\,000$.

7. Further remarks

1. By using Theorem 6 in conjunction with Table 5, we see that the largest of the "small primes", namely $p_5 = 652081$, gives rise to $652081 \cdot 3 \cdot 11 \cdot 19 \cdot 571^2$ (which has 15 decimal digits) as the larger of its two solutions to (3.5). The next Gauss prime of level 4, namely p_{131}, leads to $p_{131} \cdot 3 \cdot 7 \cdot 23 \cdot 43$, with 155 digits, as the smallest of its 26289 solutions to (3.5). The results in Section 3 show that there can be no other solutions from Gauss primes of level 4 in this gap. However, it is conceivable that there is a Gauss prime of level 5 beyond the search limit of 10^{16} which has the necessary minimum of 5 support primes, such that the resulting n leads to a solution of (3.5) and lies in the huge gap between the above 15- and 155-digit solutions. Example 3 in Section 3 shows that the second-largest Gauss prime of level 5 leads to a Gauss factorial of at least order 4; similarly, the largest Gauss prime of level 5 (see Table 4) also has only 3 support primes. Of course, a suitable Gauss prime of level 6 with a minimum of 6 support primes would also lead to a solution within the large gap.

2. Theorem 7 gives a way of constructing integers $n \equiv 1 \pmod 4$ with only one prime factor $p \equiv 1 \pmod 4$ such that $\operatorname{ord}_n \left(\frac{n-1}{4}\right)_n ! = 2$. For instance, $n = 46817 \cdot 3^2 \cdot 7 \cdot 11$ is the smallest integer with this property; see

also Example 2 in Section 3. In this case we have $\left(\frac{n-1}{4}\right)_n! = 3698542 \not\equiv -1 \pmod{n}$. This raises the question: Can we ever have

$$\left(\frac{n-1}{4}\right)_n ! \equiv -1 \pmod{n}? \tag{7.1}$$

To put this further into perspective: as we remarked following (1.3), if n has three or more distinct prime factors that are congruent to 1 modulo 4, then the left-hand side of (7.1) is always congruent to 1 (mod n). On the other hand, if n has either two or no prime factors that are congruent to 1 modulo 4, then one can find examples that satisfy (7.1). In the remaining case, however, we have the following result.

THEOREM 8. *If $n \equiv 1 \pmod 4$ has exactly one prime factor $p \equiv 1 \pmod 4$, then (7.1) has no solutions.*

PROOF. The cases $n = p^\alpha$, $n = p^\alpha q_1^{\beta_1}$, $n = p^\alpha q_1^{\beta_1} q_2^{\beta_2}$ ($q_1 \equiv q_2 \equiv -1 \pmod 4$) follow from Corollary 3(b), Theorem 5(a) and Theorem 5(b), respectively. This leaves all integers n of the form (3.4) with $r \geqq 3$. If we reduce (7.1) modulo w, then (4.19) and Lemma 5 give

$$-1 \equiv p^{\varphi(4,1,w)} \equiv p^{\varphi(w)+2^r} \pmod{w}.$$

Since $r \geqq 3$, the exponent $\varphi(w)+2^r$ is even, so -1 is a quadratic residue modulo w. This is a contradiction since w has a prime factor $q \equiv -1 \pmod 4$. □

Acknowledgement. We would like to thank Yves Gallot for generously carrying out some of the computations that led to Table 4. We also thank François Morain for verifying primality of the large Gauss primes in Tables 5 and 6.

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley (New York, 1998).
[2] J. B. Cosgrave and K. Dilcher, Extensions of the Gauss–Wilson theorem, *Integers*, **8** (2008), A39, available at http://www.integers-ejcnt.org/vol8.html.
[3] J. B. Cosgrave and K. Dilcher, Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients, *Acta Arith.*, **142** (2010), 103–118.
[4] J. B. Cosgrave and K. Dilcher, The multiplicative orders of certain Gauss factorials, *Int. J. Number Theory*, **7** (2011), 145–171.
[5] J. B. Cosgrave and K. Dilcher, An introduction to Gauss factorials, *Amer. Math. Monthly*, **118** (2011), 810–828.
[6] J. B. Cosgrave and K. Dilcher, The multiplicative orders of certain Gauss factorials, II, in preparation.

[7] R. E. Crandall, A general purpose factoring program. Perfectly Scientific – the algorithm company, available from http://www.perfsci.com/free-software.asp.
[8] L. E. Dickson, *History of the Theory of Numbers. Volume I: Divisibility and Primality*, Chelsea (New York, 1966).
[9] 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/.
[10] H. W. Gould, *Combinatorial Identities*, revised ed., Gould Publications (Morgantown, W.Va, 1972).
[11] D. H. Lehmer, The distribution of totatives, *Canad. J. Math.*, **7** (1955), 347–357.
[12] L. J. Mordell, The congruence $(p-1/2)! \equiv \pm 1 \pmod{p}$, *Amer. Math. Monthly*, **68** (1961), 145–146.
[13] F. Morain, Private communication (2006).
[14] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley (1991).
[15] The On-Line Encyclopedia of Integer Sequences, http://oeis.org/.
[16] P. Ribenboim, *The Little Book of Bigger Primes*, 2nd ed., Springer-Verlag (New York, 2004).
[17] E. W. Weisstein, Lucas Sequence. From *MathWorld* – A Wolfram Web Resource, http://mathworld.wolfram.com/LucasSequence.html.
[18] H. C. Williams, *Édouard Lucas and Primality Testing*, Wiley (1998).