THE MULTIPLICATIVE ORDERS OF CERTAIN GAUSS FACTORIALS

JOHN B. COSGRAVE AND KARL DILCHER

Abstract. A theorem of Gauss extending Wilson's theorem states the congruence $(n-1)_n! \equiv -1 \pmod{n}$ whenever n has a primitive root, and $\equiv 1 \pmod{n}$ otherwise, where $N_n!$ denotes the product of all integers up to N that are relatively prime to n. In the spirit of this theorem we study the multiplicative orders of $\left(\frac{n-1}{M}\right)_n! \pmod{n}$ for odd prime powers p^α. We prove a general result about the connection between the order for p^α and for $p^{\alpha+1}$ and study exceptions to the general rule. Particular emphasis is given to the cases $M=3$, $M=4$ and $M=6$, while the case $M=2$ is already known.

1. Introduction

The celebrated theorem of Wilson, with its converse by Lagrange, states that p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}. \tag{1.1}$$

Using the simple fact that $p-j \equiv -j \pmod{p}$ for $j=1,2,\dots,\frac{p-1}{2}$ (p an odd prime), Lagrange observed that with (1.1) we get

$$\left(\tfrac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}. \tag{1.2}$$

It is now obvious that the multiplicative order modulo p of the factorial $(\frac{p-1}{2})!$ is 4 when $p \equiv 1 \pmod{4}$, and that it can be either 1 or 2 when $p \equiv 3 \pmod{4}$. The exact determination of the latter case makes use of a class number result by Mordell [15], which implies that for any odd prime p we have

$$\operatorname{ord}_p\left(\left(\tfrac{p-1}{2}\right)!\right) = \begin{cases} 4 & \text{if} \quad p \equiv 1 \pmod{4}, \\ 2 & \text{if} \quad p \equiv 3 \pmod{4} \text{ and } h(-p) \equiv 1 \pmod{4}, \\ 1 & \text{otherwise,} \end{cases} \tag{1.3}$$

where $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. For more details, see [6].

In the recent paper [6] the authors extended (1.3) to composite moduli. This is related to Gauss' generalization of Wilson's theorem. For the statement of this and most other results in this paper it is convenient to introduce the following notation: For positive integers N and n let $N_n!$ denote the product of all integers up to N

Date: July 29, 2009.

Key words and phrases. Wilson's theorem, Gauss' theorem, factorials, congruences.

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

that are relatively prime to n, i.e.,

$$N_n! = \prod_{\substack{1\le j\le N\\ \gcd(j,n)=1}} j. \tag{1.4}$$

In our previous paper [6] we called these products *Gauss factorials*, a terminology suggested by the theorem of Gauss which states that for any integer $n\ge 2$ we have

$$(n-1)_n! \equiv \begin{cases} -1 \pmod{n} & \text{for}\quad n=2,4,p^\alpha,\ \text{or } 2p^\alpha,\\ 1 \pmod{n} & \text{otherwise,}\end{cases} \tag{1.5}$$

where p is an odd prime and α is a positive integer. Note that the first case in (1.5) indicates exactly those n that have primitive roots. For references, see [11, p. 65].

In analogy to (1.3), the authors [6] gave a complete description of the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n for odd n, and it turned out that again only the orders 1, 2, and 4 occur. In particular, in the special case where n is a power of an odd prime, we have the following (see [6, Theorem 2]).

Theorem 1. *Let p be an odd prime and α a positive integer. Then*
(1) $\operatorname{ord}_{p^\alpha}\big((\frac{p^\alpha-1}{2})_{p^\alpha}!\big)=4$ *when* $p\equiv 1 \pmod 4$*;*
(2) $\operatorname{ord}_{p^\alpha}\big((\frac{p^\alpha-1}{2})_{p^\alpha}!\big)=2$ *when*
  (a) $p>3$*,* $p\equiv 3 \pmod 4$*,* α *is odd, and* $h(-p)\equiv 1 \pmod 4$*, or*
  (a) $p>3$*,* $p\equiv 3 \pmod 4$*,* α *is even, and* $h(-p)\not\equiv 1 \pmod 4$*, or*
  (c) $p=3$ *and* α *is even;*
(3) $\operatorname{ord}_{p^\alpha}\big((\frac{p^\alpha-1}{2})_{p^\alpha}!\big)=1$ *in all other cases.*

It is the purpose of this paper to consider the more general Gauss factorials of the form

$$\left(\tfrac{p^\alpha-1}{M}\right)_{p^\alpha}! \pmod{p^\alpha},\qquad p\equiv 1 \pmod{M},\quad M\ge 2, \tag{1.6}$$

and specifically their multiplicative orders modulo p^α. It turns out that in contrast to Theorem 1 the orders generally increase as α grows. This increase is remarkably regular, and the main results of this paper concern the explanation of this. However, there are exceptions, and they are interesting in their own right, as we shall see. In [7] such Gauss factorials play a fundamental part in giving, among other things, a modulo p^3 extension of the modulo p^2 version by Chowla, Dwork, and Evans [5] of Gauss' celebrated binomial coefficient congruence.

We begin with the case $M=4$ in Section 2 since this is the easiest case in some respects. This will be extended to primes $p\equiv 3 \pmod 4$ in Section 3. In Section 4 we study the case of general $M\ge 2$, with special emphasis on $M=3$. We also present some computational results; in particular we find primes which are exceptions to the regular increase in the order as α goes from 1 to 2. In Section 5 we prove the surprising result that the exceptional primes for $M=3$ are identical with those for $M=6$. Finally in Section 6 we show that all primes p that satisfy $p^2=3x^2+3x+1$ are exceptional primes for $M=3$, and thus for $M=6$ as well.

2. The case $M=4$

The main purpose of this section is to study the orders

$$\gamma_\alpha := \operatorname{ord}_{p^\alpha}\left(\left(\tfrac{p^\alpha-1}{4}\right)_{p^\alpha}!\right) \tag{2.1}$$

for primes $p \equiv 1 \pmod 4$. Let us begin by considering the smallest example $p = 5$. Then trivially we have $\gamma_1 = 1$, and computations (with MAPLE) give $\gamma_2 = 10$, $\gamma_3 = 25$, $\gamma_4 = 250$, $\gamma_5 = 625$, and $\gamma_6 = 6250$. To explore this regularity further, we display in Table 1 the first few values of γ_α for the first five primes $p \equiv 1 \pmod 4$. The second half of the table (with $\gamma = \gamma_1$ for simplicity) shows more clearly how for a given p the order $\gamma_{\alpha+1}$ depends on γ_α.

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

Table 1: γ_α for $1 \le \alpha \le 5$ and $p \le 37$, $p \equiv 1 \pmod 4$.

Supported by further computations one would be tempted to conjecture that for primes $p \equiv 1 \pmod 4$ and $\gamma := \operatorname{ord}_p(\frac{p-1}{4}!)$ the sequence of orders $\gamma_1 = \gamma, \gamma_2, \gamma_3, \dots$ is

$$\begin{cases} \gamma, p\gamma, p^2\gamma, p^3\gamma, \dots & \text{when } p \equiv 1 \pmod 8 \\ & \quad \text{or } p \equiv 5 \pmod 8 \text{ and } 4|\gamma, \\ \gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \dots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \equiv 2 \pmod 4, \\ \gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \dots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \text{ is odd.} \end{cases} \tag{2.2}$$

However, it turns out that for $p = 29\,789$ we have $\gamma_1 = 14\,894$, while $\gamma_2 = 7\,447$. In this section we will prove the pattern (2.2), and shed some light on the exceptional primes (such as the above $p = 29\,789$) and on the conditions under which they occur.

For the results and proofs we need the following objects. Let p be an odd prime. Then for an integer $a \ge 2, p \nmid a$, the *Fermat quotient to base a* is defined by

$$q_p(a) := \frac{a^{p-1} - 1}{p}, \tag{2.3}$$

while the *Wilson quotient* is defined by

$$w_p := \frac{(p-1)! + 1}{p}. \tag{2.4}$$

Both quotients are obviously integers, by Fermat's little theorem and Wilson's theorem. These quotients are of some importance in the classical theory surrounding Fermat's last theorem; see, e.g., [17]. We will also need a generalization of the Wilson quotient, namely

$$W(n) := \frac{(n-1)_n! \pm 1}{n}, \tag{2.5}$$

with the sign chosen according to whether or not n has a primitive root; see (1.5). It is clear that $W(p)=w_p$. These quotients were studied in detail in [2].

The Fermat quotients enter the picture through the following congruences.

Lemma 1. *For all primes $p\geq 5$ we have*

$$\sum_{j=1}^{p-1}\frac{1}{j}\equiv 0\pmod{p^2}, \tag{2.6}$$

$$\sum_{j=1}^{\frac{p-1}{2}}\frac{1}{j}\equiv -2q_p(2)\pmod{p}\qquad(\textit{for}\quad p\geq 3), \tag{2.7}$$

$$\sum_{j=1}^{\lfloor\frac{p-1}{4}\rfloor}\frac{1}{j}\equiv -3q_p(2)\pmod{p}. \tag{2.8}$$

Congruences of this type were obtained by several authors in the early 1900s, with the most extensive and general treatment in a paper by Emma Lehmer [13]. The congruences (41) and (43) in that paper, which are given modulo p^2, immediately reduce to (2.7) and (2.8), respectively, when taken modulo p, and (2.6) follows as a special case from a congruence in [13, p. 353].

Since clearly

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

we will use the simpler form on the right-hand side for the remainder of this paper. All further results are based on the following

Proposition 2.1. *For any prime $p\equiv 1\pmod 4$ and positive integer α we have*

$$\left(\tfrac{p^{\alpha+1}-1}{4}\right)_p!\equiv(-1)^{\frac{p-1}{4}}\left(\tfrac{p^\alpha-1}{4}\right)_p!\left(1+\frac{1}{4}p^\alpha\big(W(p^\alpha)+3q_p(2)\big)\right)\pmod{p^{\alpha+1}} \tag{2.9}$$

Proof. If we note that

$$\tfrac{p^{\alpha+1}-1}{4}=\tfrac{p-1}{4}p^\alpha+\tfrac{p^\alpha-1}{4},$$

then we see that with $r:=(p-1)/4$ we have

$$\begin{aligned}\left(\tfrac{p^{\alpha+1}-1}{4}\right)_p! &=\prod_{j=0}^{r-1}\big[(jp^\alpha+1)(jp^\alpha+2)\dots(jp^\alpha+p^\alpha-1)\big]^*\\ &\quad\times\big[(rp^\alpha+1)\dots(rp^\alpha+\tfrac{p^\alpha-1}{4})\big]^*,\end{aligned} \tag{2.10}$$

where $[\dots]^*$ indicates that multiples of p are excluded from the product. Expanding these products, we first get for $0\leq j\leq r-1$,

$$\big[(jp^\alpha+1)\dots(jp^\alpha+p^\alpha-1)\big]^*\equiv\big[1\cdot2\cdot\ldots\cdot(p^\alpha-1)\big]^*\big(1+jp^\alpha\sum_{\substack{i=1\\ p\nmid i}}^{p^\alpha-1}\frac{1}{i}\big)\pmod{p^{\alpha+1}}.$$

The summation on the right-hand side is, modulo p, just $p^{\alpha-1}$ copies of the sum (2.6), which vanishes modulo p. Thus we have for all j, $0\leq j\leq r-1$,

$$\big[(jp^\alpha+1)\dots(jp^\alpha+p^\alpha-1)\big]^*\equiv(p^\alpha-1)_p!\pmod{p^{\alpha+1}}. \tag{2.11}$$

Similarly, we expand

$$\big[(rp^\alpha+1)\dots(rp^\alpha+\tfrac{p^\alpha-1}{4})\big]^*\equiv\Big(\tfrac{p^\alpha-1}{4}\Big)_p!\big(1+rp^\alpha\sum_{\substack{i=1\\ p\nmid i}}^{\frac{p^\alpha-1}{4}}\frac{1}{i}\big)\pmod{p^{\alpha+1}}. \tag{2.12}$$

Now, since

$$\tfrac{p^\alpha-1}{4}=\tfrac{p^{\alpha-1}-1}{4}p+\tfrac{p-1}{4},$$

we have, again using (2.6) and then (2.8),

$$\sum_{\substack{i=1\\ p\nmid i}}^{\frac{p^\alpha-1}{4}}\frac{1}{i}\equiv\sum_{i=1}^{\frac{p-1}{4}}\frac{1}{i}\equiv-3q_p(2)\pmod{p}, \tag{2.13}$$

so that

$$\big[(rp^\alpha+1)\dots(rp^\alpha+\tfrac{p^\alpha-1}{4})\big]^*\equiv\left(\frac{p^\alpha-1}{4}\right)_p!\,(1-3rq_p(2)p^\alpha)\pmod{p^{\alpha+1}}. \tag{2.14}$$

Next, by (2.5) we have

$$(p^\alpha-1)_p!=-1+W(p^\alpha)p^\alpha, \tag{2.15}$$

and therefore, with a binomial expansion,

$$((p^\alpha-1)_p!)^r\equiv(-1)^r\,(1-rW(p^\alpha)p^\alpha)\pmod{p^{\alpha+1}}.$$

This, together with (2.11), (2.14) and (2.10) gives

$$\begin{aligned}\Big(\tfrac{p^{\alpha+1}-1}{4}\Big)_p!&\equiv(-1)^r\Big(\tfrac{p^\alpha-1}{4}\Big)_p!\,(1-3rq_p(2)p^\alpha)\,(1-rW(p^\alpha)p^\alpha)\\&\equiv(-1)^r\Big(\tfrac{p^\alpha-1}{4}\Big)_p!\,\big(1-rp^\alpha\big(W(p^\alpha)+3q_p(2)\big)\big)\pmod{p^{\alpha+1}}.\end{aligned}$$

Finally we note that $rp^\alpha\equiv-\frac{1}{4}p^\alpha\pmod{p^{\alpha+1}}$, and (2.9) follows immediately from the last line. □

Before we can state the main result of this section, we need to introduce another arithmetic function, similar to the Wilson quotient. Given the prime power p^α, we define $V(p^\alpha)$ by

$$\left(\Big(\tfrac{p^\alpha-1}{4}\Big)_p!\right)^{\gamma_\alpha}\equiv1+V(p^\alpha)p^\alpha\pmod{p^{\alpha+1}}, \tag{2.16}$$

where γ_α is defined by (2.1).

Proposition 2.2. *Let $p\equiv1\pmod 4$ be a prime, and for $\alpha\ge1$ let γ_α be defined as in (2.1). If $p\equiv1\pmod 8$, then*

$$\gamma_{\alpha+1}=p\gamma_\alpha\quad\textit{or}\quad\gamma_{\alpha+1}=\gamma_\alpha. \tag{2.17}$$

If $p\equiv5\pmod 8$, then

$$\gamma_{\alpha+1}=\begin{cases}p\gamma_\alpha\quad\textit{or}\quad\gamma_\alpha & \textit{when}\quad\gamma_\alpha\equiv0\pmod 4,\\ \frac{1}{2}p\gamma_\alpha\quad\textit{or}\quad\frac{1}{2}\gamma_\alpha & \textit{when}\quad\gamma_\alpha\equiv2\pmod 4,\\ 2p\gamma_\alpha\quad\textit{or}\quad2\gamma_\alpha & \textit{when}\quad\gamma_\alpha\equiv1\pmod 2.\end{cases} \tag{2.18}$$

In all cases the first alternative holds if and only if

$$T(p^\alpha):=V(p^\alpha)+\tfrac{1}{4}\gamma_\alpha w_p+\tfrac{3}{4}\gamma_\alpha q_p(2)\not\equiv0\pmod{p}. \tag{2.19}$$

Proof. When $p \equiv 1 \pmod 8$, then $(-1)^{\frac{p-1}{4}} = 1$, and with (2.9) and (2.16) we get

$$\begin{aligned}\Big(\big(\tfrac{p^{\alpha+1}-1}{4}\big)_p!\Big)^{\gamma_\alpha} &\equiv \big(1+V(p^\alpha)p^\alpha\big)\Big(1+\frac{p^\alpha}{4}\big(W(p^\alpha)+3q_p(2)\big)\Big)^{\gamma_\alpha} \\ &\equiv 1+p^\alpha T(p^\alpha) \pmod{p^{\alpha+1}}.\end{aligned} \tag{2.20}$$

Hence the order $\gamma_{\alpha+1}$ is equal to γ_α when

$$T(p^\alpha) \equiv 0 \pmod p. \tag{2.21}$$

holds. If (2.21) does not hold, then raising both sides of (2.20) to the power p gives

$$\Big(\big(\tfrac{p^{\alpha+1}-1}{4}\big)_p!\Big)^{p\gamma_\alpha} \equiv 1 \pmod{p^{\alpha+1}}.$$

Since p is a prime and γ_α is the order of the previous Gauss factorial, no smaller powers give $\equiv 1 \pmod{p^{\alpha+1}}$, which means that the order is $p\gamma_\alpha$; this gives (2.17).

Let now $p \equiv 5 \pmod 8$. First, if γ_α is even, then we have with (2.16),

$$\Big(\big(\tfrac{p^{\alpha}-1}{4}\big)_p!\Big)^{\gamma_\alpha/2} \equiv -\big(1+\tfrac{1}{2}V(p^\alpha)p^\alpha\big) \pmod{p^{\alpha+1}}.$$

With (2.9) and the fact that $(-1)^{\frac{p-1}{4}} = -1$ we then have, after evaluating a product as we did in (2.20),

$$\Big(\big(\tfrac{p^{\alpha+1}-1}{4}\big)_p!\Big)^{\gamma_\alpha/2} \equiv (-1)^{1+\gamma_\alpha/2}\big(1+\tfrac{1}{2}p^\alpha T(p^\alpha)\big) \pmod{p^{\alpha+1}}. \tag{2.22}$$

This means that for $1+\gamma_\alpha/2$ even, i.e., when $\gamma_\alpha \equiv 2 \pmod 4$, the order is $\frac{1}{2}\gamma_\alpha$ when (2.21) holds, or $\frac{1}{2}\gamma_\alpha p$ otherwise. On the other hand, when $\gamma_\alpha \equiv 0 \pmod 4$ then both sides of (2.22) need to be squared, and with the same argument as before we get $\gamma_{\alpha+1} = \gamma_\alpha$ or $p\gamma_\alpha$.

Finally, when γ_α is odd, then both sides of (2.9) need to be raised to the power $2\gamma_\alpha$; the details are the same as before. We then get $\gamma_{\alpha+1} = 2\gamma_\alpha$ or $2p\gamma_\alpha$.

To complete the proof, we simplify the congruence (2.21), using the fact that $W(p^n) \equiv W(p^{n-1}) \pmod{p^{n-1}}$ for all $n \geq 2$ and $p \geq 5$ (see [2, Prop. 3.1]), so that $W(p^n) \equiv w_p \pmod p$. With this, (2.21) leads to (2.19), and the proof is complete. □

It is also interesting to consider the sequence of orders $\gamma_1, \gamma_2, \dots$ for a fixed prime p. Proposition 2.2 immediately gives the following

Corollary 1. *Let $p \equiv 1 \pmod 4$ and $\gamma := \mathrm{ord}_p(\frac{p-1}{4}!)$. Then the sequence of orders $\gamma_1 = \gamma, \gamma_2, \gamma_3, \dots$ is as given in* (2.2). *In each case the power of p will increase by 1 only when the congruence* (2.19) *holds.*

Remark. While the condition (2.19) is usually satisfied, it can happen that the expression on the left vanishes modulo p. This is indeed the case for $p = 29\,789$, and we find in this case that $\gamma_1 = 14\,894$, while $\gamma_2 = 7\,447$. No other such case was found for $p \leq 4\times 10^8$. It is reasonable to expect a similar behaviour for the number of zeros modulo p as in the case of the Fermat and Wilson quotients, namely roughly $\log\log n$ for primes up to n, which is based on the (unproven) assumption that the values of the Fermat and Wilson quotients are uniformly distributed modulo p. For more details on this, see [9].

3. $M = 4$ and $p \equiv 3 \pmod 4$

In this section and the following one we generalize Propositions 2.1 and 2.2 in two different directions: First we consider also primes $p \equiv 3 \pmod 4$, and then we study the Gauss factorials $\big(\frac{p^\alpha-1}{M}\big)_p!$ for any integer $M \geq 2$.

We begin with the first generalization. While $\big(\frac{p^\alpha-1}{4}\big)_p!$ does not make sense when $p \equiv 3 \pmod 4$ and α is odd, the expression $\lfloor\frac{p^\alpha-1}{4}\rfloor_p!$ is defined for all p and α. We begin with a lemma that extends the sum (2.8).

Lemma 2. *For all odd primes p and positive integers α we have*

$$\sum_{j=1}^{\lfloor\frac{p^\alpha-1}{4}\rfloor} \frac{1}{j} \equiv -3q_p(2) \pmod p. \tag{3.1}$$

Proof. When $p \equiv 1 \pmod 4$, this is just (2.13). Let now $p \equiv 3 \pmod 4$. When α is odd then we have

$$\lfloor\tfrac{p^\alpha-1}{4}\rfloor = \tfrac{p^\alpha-3}{4} = \tfrac{p^{\alpha-1}-1}{4}p + \tfrac{p-3}{4}. \tag{3.2}$$

This means that the sum in (3.1) runs through a certain number of reduced residue classes modulo p, followed by a sum from 1 to $(p-3)/4$ which, by (2.8), is congruent to $-3q_p(2)$. On the other hand, when α is even, then we have

$$\lfloor\tfrac{p^\alpha-1}{4}\rfloor = \tfrac{p^\alpha-1}{4} = \tfrac{p^{\alpha-1}-3}{4}p + \tfrac{3p-1}{4}, \tag{3.3}$$

which means that this time we have a "remainder sum" ranging from 1 to $(3p-1)/4$. We evaluate it as follows:

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

where we have once again used (2.6) and (2.8). This completes the proof of the lemma. □

We are now ready to prove the following result which supplements Proposition 2.1.

Proposition 3.1. *For any prime $p \equiv 3 \pmod 4$ and positive integer α we have*

$$\lfloor\tfrac{p^{\alpha+1}-1}{4}\rfloor_p! \equiv \frac{-1}{\lfloor\frac{p^\alpha-1}{4}\rfloor_p!\,\big(1+\frac{1}{4}p^\alpha\big(W(p^\alpha)+3q_p(2)\big)\big)} \pmod{p^{\alpha+1}} \tag{3.4}$$

Proof. Following the outline of the proof of Proposition 2.1, we note that

$$\lfloor\tfrac{p^{\alpha+1}-1}{4}\rfloor = \tfrac{p+1}{4}p^\alpha + \lfloor\tfrac{p^\alpha+3}{4}\rfloor,$$

and with $s := (p+1)/4$ this corresponds to

$$\lfloor\tfrac{p^{\alpha+1}-1}{4}\rfloor_p! = \frac{\prod_{j=0}^{s-1}\big[(jp^\alpha+1)(jp^\alpha+2)\dots(jp^\alpha+p^\alpha-1)\big]^*}{\big[(sp^\alpha-1)\dots(sp^\alpha-\lfloor\frac{p^\alpha-1}{4}\rfloor)\big]^*}. \tag{3.5}$$

As in (2.12) we get, with Lemma 2,

$$\begin{aligned}\big[(sp^\alpha-1)\dots(sp^\alpha-\tfrac{p^\alpha-1}{4})\big]^* &\equiv (-1)^\beta \lfloor\tfrac{p^\alpha-1}{4}\rfloor_p!\big(1-sp^\alpha\sum_{\substack{j=1\\ p\nmid j}}^{\lfloor\frac{p^\alpha-1}{4}\rfloor}\frac{1}{j}\big) \pmod{p^{\alpha+1}}\\ &\equiv (-1)^\beta \lfloor\tfrac{p^\alpha-1}{4}\rfloor_p!\big(1+\tfrac{3}{4}p^\alpha q_p(2)\big) \pmod{p^{\alpha+1}},\end{aligned}$$

where β is the number of terms in the product on the left, to be determined later. Hence with (2.15) we get from (3.5),

$$\begin{aligned}\lfloor\tfrac{p^{\alpha+1}-1}{4}\rfloor_p! &\equiv \frac{(-1)^s\big(1-sp^\alpha W(p^\alpha)\big)}{(-1)^\beta\lfloor\frac{p^\alpha-1}{4}\rfloor_p!\big(1+\frac{3}{4}p^\alpha q_p(2)\big)} \pmod{p^{\alpha+1}}\\ &\equiv \frac{(-1)^{\beta+s}}{\lfloor\frac{p^\alpha-1}{4}\rfloor_p!\big(1+\frac{1}{4}p^\alpha\big(W(p^\alpha)+3q_p(2)\big)\big)} \pmod{p^{\alpha+1}},\end{aligned}$$

where we have used the fact that $(1-sp^\alpha W(p^\alpha))\equiv(1+\frac{1}{4}p^\alpha W(p^\alpha)) \pmod{p^{\alpha+1}}$. Finally, to determine β, we note that by (3.2) and (3.3), and keeping in mind that a reduced residue system modulo p has an even number of elements, the parity of β is the same as that of $(p-3)/4$, resp. $(3p-1)/4$. But clearly,

$$\tfrac{p-3}{4}-\tfrac{p+1}{4}=-1, \qquad \tfrac{3p-1}{4}+\tfrac{p+1}{4}=p,$$

and therefore $\beta+s$ is odd, which completes the proof of (3.4). □

For the next result, which is completely analogous to Proposition 2.2, we let γ_α and $V(p^\alpha)$ be defined as in (2.1) and (2.16), with the inner-most parentheses replaced by the greatest-integer brackets $\lfloor\dots\rfloor$.

Proposition 3.2. *Let $p\equiv 3 \pmod 4$ be a prime and α a positive integer. Then*

$$\gamma_{\alpha+1}=\begin{cases}\frac{1}{2}p\gamma_\alpha \quad \textit{or} \quad \frac{1}{2}\gamma_\alpha & \textit{when } \gamma_\alpha \textit{ is even},\\ 2p\gamma_\alpha \quad \textit{or} \quad 2\gamma_\alpha & \textit{when } \gamma_\alpha \textit{ is odd}.\end{cases}$$

In both cases the first alternative holds if and only if

$$V(p^\alpha)+\tfrac{1}{4}\gamma_\alpha w_p+\tfrac{3}{4}\gamma_\alpha q_p(2)\not\equiv 0 \pmod p. \tag{3.6}$$

α/p	3	7	11	19	23	31
1	1	1	10	9	22	15
2	6	14	55	342	253	930
3	9	49	1 210	3 249	11 538	14,415
4	54	686	6 655	123 462	133 837	893 730
5	81	2 401	146 410	1 172 889	6 156 502	13 852 815

Table 2: γ_α for $1\le\alpha\le 5$ and $p\le 31$, $p\equiv 3 \pmod 4$.

The proof of Proposition 3.2 is very similar to that of Proposition 2.2; we therefore leave out the details. The reason for the simpler statement of Proposition 3.2 lies in the fact that the sign on the right-hand side of (3.4) does not depend on p, as it does in (2.9).

Since the order $\gamma:=\gamma_1$ has to divide $p-1$, where $p\equiv 3 \pmod 4$, γ is either odd or $\gamma\equiv 2 \pmod 4$. In the former case we have $2\gamma\equiv 2 \pmod 4$, and in the latter case $\frac{1}{2}\gamma$ is odd. This means that in contrast to Corollary 1 and (2.2) we have the following simpler situation, which is illustrated in Table 2.

Corollary 2. *With p and $\gamma=\gamma_1$ as above, the sequence of orders $\gamma_1,\gamma_2,\gamma_3,\ldots$ is*

$$\begin{cases}\gamma,\frac{1}{2}p\gamma,p^2\gamma,\frac{1}{2}p^3\gamma,\ldots & \textit{when } \gamma \textit{ is even,,}\\ \gamma,2p\gamma,p^2\gamma,2p^3\gamma,\ldots & \textit{when } \gamma \textit{ is odd.}\end{cases}$$

In each case the power of p will increase by 1 only when the congruence (3.6) *holds.*

4. General $M\geq 2$

We now turn to the second type of generalization. Let $M\geq 2$ be an integer. Our goal now is to study

$$\gamma_\alpha^{(M)} := \mathrm{ord}_{p^\alpha}\left(\left(\tfrac{p^\alpha-1}{M}\right)_{p^\alpha}!\right), \tag{4.1}$$

for primes $p\equiv 1 \pmod{M}$. We note in passing that primes in other classes modulo M could also be considered, in the spirit of Propositions 3.1 and 3.2. However, for the sake of simplicity we restrict our attention to the main case $p\equiv 1 \pmod{M}$.

While there are a few other evaluations of sums of the type (2.6)–(2.8) (see Lemma 3 below), in general such congruences do not exist. We therefore denote

$$S_M(p) := \sum_{j=1}^{\frac{p-1}{M}}\frac{1}{j} \pmod{p}. \tag{4.2}$$

We now have the following analogue of Proposition 2.1.

Proposition 4.1. *Let $M\geq 2$ be an integer. For any prime $p\equiv 1 \pmod{M}$ and positive integer α we have*

$$\left(\tfrac{p^{\alpha+1}-1}{M}\right)_p! \equiv (-1)^{\frac{p-1}{M}}\left(\tfrac{p^\alpha-1}{M}\right)_p!\left(1+\frac{1}{M}p^\alpha\big(W(p^\alpha)-S_M(p)\big)\right) \pmod{p^{\alpha+1}} \tag{4.3}$$

The proof is almost verbatim the same as that of Proposition 2.1, with the only difference that the sum $S_M(p)$ is not evaluated. If in analogy to (2.16) we define $V_M(p^\alpha)$ by

$$\left(\left(\tfrac{p^\alpha-1}{M}\right)_p!\right)^{\gamma_\alpha^{(M)}} \equiv 1+V_M(p^\alpha)p^\alpha \pmod{p^{\alpha+1}}, \tag{4.4}$$

then we have the following result which is analogous to Proposition 2.2.

Proposition 4.2. *Let $M\geq 2$ be an integer, let $p\equiv 1 \pmod{M}$ be a prime, and for $\alpha\geq 1$ let $\gamma_\alpha^{(M)}$ be defined as in* (4.1). *If $p\equiv 1 \pmod{2M}$, then*

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

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

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

In all cases the first alternative holds if and only if

$$T_\alpha^{(M)}(p) := V_M(p^\alpha)+\tfrac{1}{M}\gamma_\alpha^{(M)}\big(w_p-S_M(p)\big)\not\equiv 0 \pmod{p}. \tag{4.5}$$

The proof is identical with that of Proposition 2.2. However, it is worth pointing out that for odd M only the first case can occur since obviously $p \equiv M+1 \pmod{2M}$ is impossible for odd primes p.

We now consider a few special cases. When $M=2$, we know by Theorem 1 that $\gamma_\alpha^{(2)} = 4$ for all α. This means that by Proposition 4.2 we have $T_\alpha^{(2)}(p) \equiv 0 \pmod{p}$ for all $\alpha \geq 1$ or, with (2.7),

$$V_2(p^\alpha) \equiv -2w_p - 4q_p(2),$$

and with (4.4) we obtain

$$\left(\left(\tfrac{p^\alpha-1}{2}\right)_p!\right)^4 \equiv 1-(2w_p+4q_p(2))p^\alpha \pmod{p^{\alpha+1}}.$$

This immediately implies

Corollary 3. *For any prime $p \equiv 1 \pmod{4}$ and positive integer α we have*

$$\left(\left(\tfrac{p^\alpha-1}{2}\right)_p!\right)^2 \equiv -1+(w_p+2q_p(2))p^\alpha \pmod{p^{\alpha+1}},$$

and in particular

$$\left(\tfrac{p-1}{2}!\right)^2 \equiv -1+(w_p+2q_p(2))p \pmod{p^2}.$$

This last congruence raises the question whether $w_p+2q_p(2) \equiv 0 \pmod{p}$ can occur. Computations show that the only prime $p \equiv 1 \pmod{4}$ and $p < 2\cdot 10^8$ for which this happens is $p=53$. (Four other small primes, namely 3, 11, 31 and 47 satisfy this congruence up to 10^6, but they are $\equiv 3 \pmod{4}$.)

For the next special cases we require another supplement to Lemma 1.

Lemma 3. *For all primes $p \geq 5$ we have*

$$\sum_{j=1}^{\lfloor\frac{p-1}{3}\rfloor} \frac{1}{j} \equiv -\tfrac{3}{2}q_p(3) \pmod{p}, \tag{4.6}$$

and for $p \geq 7$,

$$\sum_{j=1}^{\lfloor\frac{p-1}{6}\rfloor} \frac{1}{j} \equiv -2q_p(2)-\tfrac{3}{2}q_p(3) \pmod{p}. \tag{4.7}$$

As was the case with Lemma 1, these two congruences follow directly from modulo p^2 congruences in [13], here from (42) and (44), respectively.

We can now state as special case of Proposition 4.2 the following result which is analogous to Propositions 2.2 and 3.2.

Proposition 4.3. *Let $p \equiv 1 \pmod{3}$ be a prime and α a positive integer. Then $\gamma_{\alpha+1}^{(3)} = p\gamma_\alpha^{(3)}$ when*

$$V_3(p^\alpha)+\tfrac{1}{3}\gamma_\alpha^{(3)}\left(w_p+\tfrac{3}{2}q_p(3)\right) \not\equiv 0 \pmod{p}, \tag{4.8}$$

and $\gamma_{\alpha+1}^{(3)} = \gamma_\alpha^{(3)}$ otherwise.

Calculations show that exceptional primes, i.e., those for which (4.8) does not hold, are 13, 181, 2 521, 76 543, 489 061, and 6 811 741. These are all up to $4\cdot 10^8$.

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

Table 3: Exceptional primes $p < 2 \cdot 10^6$ for $3 \leq M \leq 100$.

A criterion similar to (4.8) can be established for $M = 6$, using the congruence (4.7). The case $M = 4$ has also been tested up to $4 \cdot 10^8$, and $p = 29\,789$ is the only exceptional prime found. For all other M we carried the calculations up to $2 \cdot 10^6$ only. Table 3 shows all exceptional primes $p < 2 \cdot 10^6$ for $3 \leq M \leq 100$.

5. Exceptional primes for $M = 3$ and $M = 6$

Table 3 suggests that the exceptional primes for $M = 6$ are the same as those for $M = 3$. This is indeed true, and is an immediate consequence of the following rather surprising result, a proof of which is the main purpose of this section.

Proposition 5.1. *For any prime* $p \equiv 1 \pmod 6$ *we have*

$$\gamma_1^{(3)} T_1^{(6)}(p) \equiv 2\gamma_1^{(6)} T_1^{(3)}(p) \pmod{p}. \tag{5.1}$$

The main ingredient in the proof of this result is the following lemma which we will prove later.

Lemma 4. *For any prime* $p \equiv 1 \pmod 6$ *we have*

$$\frac{\left(\frac{p-1}{6}!\right)^{p-1}}{\left(\frac{p-1}{3}!\right)^{2(p-1)}} \equiv 1 - \frac{p}{2}\left(w_p + \frac{3}{2}q_p(3) - \frac{2}{3}q_p(2)\right) \pmod{p^2}. \tag{5.2}$$

Proof of Proposition 5.1. The expression $T_1^{(3)}(p)$ is given by the left-hand side of (4.8), and similarly with (4.5) and (4.7) we get

$$T_1^{(6)}(p) = V_6(p) + \tfrac{1}{6}\gamma_1^{(6)}\left(w_p + \tfrac{3}{2}q_p(3) + 2q_p(2)\right).$$

After some simplification we see that (5.1) is equivalent to the congruence

$$\begin{aligned} \gamma_1^{(3)} V_6(p) - 2\gamma_1^{(6)} V_3(p) \equiv {} & \frac{1}{2}\gamma_1^{(3)}\gamma_1^{(6)}\left(w_p + \tfrac{3}{2}q_p(3)\right) \\ & - \frac{1}{6}\gamma_1^{(3)}\gamma_1^{(6)} 2q_p(2) \pmod{p}. \end{aligned}$$

We now divide both sides by $\gamma_1^{(3)}\gamma_1^{(6)}$, which is allowable since, as orders modulo M, these numbers satisfy $1 \leq \gamma_1^{(M)} \leq p-1$. Hence (5.1) is equivalent to

$$\frac{V_6(p)}{\gamma_1^{(6)}} - 2\frac{V_3(p)}{\gamma_1^{(3)}} \equiv \frac{1}{2}\left(w_p + \tfrac{3}{2}q_p(3)\right) - \frac{1}{3}q_p(2) \pmod{p}. \tag{5.3}$$

To prove (5.3), we first use the definition (4.4) with $\alpha = 1$ and $M = 3$, and for simplicity we set $\gamma := \gamma_1^{(3)}$. Then

$$\begin{aligned}\left(\frac{p-1}{3}!\right)^{p-1} &= \left(\left(\frac{p-1}{3}!\right)^{\gamma}\right)^{\frac{p-1}{\gamma}} \\ &\equiv (1+pV_3(p))^{\frac{p-1}{\gamma}} \equiv 1+\frac{p-1}{\gamma}pV_3(p) \pmod{p^2},\end{aligned}$$

so that

$$\left(\frac{p-1}{3}!\right)^{p-1} \equiv 1-\frac{1}{\gamma_1^{(3)}}pV_3(p) \pmod{p^2},$$

and similarly

$$\left(\frac{p-1}{6}!\right)^{p-1} \equiv 1-\frac{1}{\gamma_1^{(6)}}pV_6(p) \pmod{p^2}.$$

With these last two congruences, and using the fact that $(1-ap)^{-1} \equiv 1+ap \pmod{p^2}$, we obtain

$$\begin{aligned}\frac{\left(\frac{p-1}{6}!\right)^{p-1}}{\left(\frac{p-1}{3}!\right)^{2(p-1)}} &\equiv \left(1-\frac{p}{\gamma_1^{(6)}}V_6(p)\right)\left(1+2\frac{p}{\gamma_1^{(3)}}V_3(p)\right) \pmod{p^2} \\ &\equiv 1-\frac{p}{\gamma_1^{(6)}}V_6(p)+2\frac{p}{\gamma_1^{(3)}}V_3(p) \pmod{p^2}.\end{aligned}$$

This, together with (5.2), gives (5.3), which completes the proof of Proposition 5.1.
□

Remark. The congruence (5.1) can obviously be written as $T_1^{(6)}(p)/T_1^{(3)}(p) \equiv 2\cdot\gamma_1^{(6)}/\gamma_1^{(3)} \pmod{p}$. Here the right-hand side is defined, as rational number, for all primes $p \equiv 1 \pmod{6}$, including the exceptional primes. Surprisingly, for $p < 10^6$ only the following 18 values of $\gamma_1^{(6)}/\gamma_1^{(3)}$, occuring with different frequencies, have been observed:

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

Note the multiplicative symmetry of this set about $\frac{1}{2}$. A further investigation of this is part of a forthcoming paper [8] by the authors.

In order to prove Lemma 4, we use some deep results from [3], related to Jacobi sums. In particular, we use the fact that a prime $p \equiv 1 \pmod{6}$ has the unique (up to signs) representation $p = a^2 + 3b^2$. In what follows, the signs of a and b are crucial and require some explanation (see [3, pp. 103–106]):

Let g be a primitive root modulo p and χ a character modulo p of order 6 with $\chi(g) = e^{2\pi i/6} = (1+i\sqrt{3})/2$. Then the Jacobi sum J evaluates as $J(\chi,\chi^2) = a + ib\sqrt{3}$, where the integers a and b satisfy $p = a^2+3b^2$, and their signs are fixed by the congruences

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

With the integers a and b thus determined, we define two closely related integers r and u as follows. Let $Z = \text{ind}_g 2$, the index of 2 $\pmod{p}$ with respect to g. Then

$$\begin{cases} r = 2a, \quad u = 2a & \text{when} \quad Z \equiv 0 \pmod{3}, \\ r = -a - 3b, \quad u = -a + 3b & \text{when} \quad Z \equiv 1 \pmod{3}, \\ r = -a + 3b, \quad u = -a - 3b & \text{when} \quad Z \equiv 2 \pmod{3}. \end{cases} \tag{5.4}$$

Now we set $p = 6f + 1$ and quote the following congruences from Theorem 9.4.4 in [3, p. 283], rewritten in terms of the Fermat quotients defined in (2.3):

$$\binom{2f}{f} \equiv (-1)^{f+1}\left(u - \frac{p}{u}\right)\left(1 + \frac{2}{3}pq_p(2)\right) \pmod{p^2}, \tag{5.5}$$

$$\binom{4f}{2f} \equiv -r + \frac{p}{r} \pmod{p^2}, \tag{5.6}$$

$$\binom{6f}{2f} \equiv 1 + \frac{3}{2}pq_p(3) \pmod{p^2}. \tag{5.7}$$

Furthermore, by (2.4) we have

$$(6f)! \equiv -1 + pw_p \pmod{p^2}.$$

Using these four congruences, we get

$$\begin{aligned} \frac{f!^2}{(2f)!^4} &= \frac{f!^2}{(2f)!} \cdot \frac{(4f)!}{(2f)!^2} \cdot \frac{(6f)!}{(4f)!(2f)!} \cdot \frac{1}{(6f)!} = \frac{\binom{4f}{2f}\binom{6f}{2f}}{\binom{2f}{f}(6f)!} \\ &\equiv (-1)^{f+1}\frac{r - \frac{p}{r}}{u - \frac{p}{u}} \cdot \frac{1 + \frac{3}{2}pq_p(3)}{(1 + \frac{2}{3}pq_p(2))(1 - pw_p)} \pmod{p^2} \\ &\equiv (-1)^{f+1}\frac{r - \frac{p}{r}}{u - \frac{p}{u}}(1 + \frac{3}{2}pq_p(3))(1 - \frac{2}{3}pq_p(2))(1 + pw_p) \pmod{p^2} \\ &\equiv (-1)^{f+1}\frac{r - \frac{p}{r}}{u - \frac{p}{u}}\big(1 + p\big(w_p + \frac{3}{2}q_p(3) - \frac{2}{3}q_p(2)\big)\big) \pmod{p^2}. \end{aligned}$$

Now we raise both sides to the power $\frac{p-1}{2}$ and note that in

$$(f+1)\frac{p-1}{2} = \left(\frac{p-1}{6} + 1\right)\left(3\frac{p-1}{6}\right)$$

one factor is always even, so that the power of -1 disappears. Furthermore, we have for any integer A,

$$(1 + pA)^{\frac{p-1}{2}} \equiv 1 + \frac{p-1}{2}pA \equiv 1 - \frac{p}{2}A \pmod{p^2},$$

and therefore

$$\frac{\left(\frac{p-1}{6}!\right)^{p-1}}{\left(\frac{p-1}{3}!\right)^{2(p-1)}} \equiv \left(\frac{r - \frac{p}{r}}{u - \frac{p}{u}}\right)^{\frac{p-1}{2}} \big(1 - \frac{p}{2}\big(w_p + \frac{3}{2}q_p(3) - \frac{2}{3}q_p(2)\big)\big) \pmod{p^2}. \tag{5.8}$$

To complete the proof of Lemma 4, we require the following lemma.

Lemma 5. *Let $p \equiv 1 \pmod{6}$ and r, u be defined as in (ii) and (iii) above. Then*

$$\left(r - \frac{p}{r}\right)^{p-1} \equiv \left(u - \frac{p}{u}\right)^{p-1} \pmod{p^2}. \tag{5.9}$$

If we set $Q := (r - \frac{p}{r})/(u - \frac{p}{u})$, then (5.9) obviously shows that $Q^{p-1} \equiv 1 \pmod{p^2}$. Now, the modular square root is unique up to sign in this case, and so $Q^{(p-1)/2} \equiv 1 \pmod{p^2}$ since the left-hand side of (5.8) is $\equiv 1 \pmod{p}$ by Fermat's little theorem. Hence (5.2) follows from (5.8).

Proof of Lemma 5. For a given prime $p \equiv 1 \pmod{6}$ we consider the three cases in (5.4). In the first case the congruence (5.9) is trivial. In the other two cases we first note that

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

Now, using the fact that the exponents $p-1$ and $p-3$ are even, we see that (5.9) follows if we can show that

$$(a+3b)^{p-1} - (a-3b)^{p-1} + p\big((a+3b)^{p-3} - (a-3b)^{p-3}\big) \equiv 0 \pmod{p^2}. \tag{5.10}$$

The main ingredient in the proof of this congruence is the binomial expansion

$$(a+3b)^{p-\nu} - (a-3b)^{p-\nu} = 6ab \sum_{j=0}^{\frac{p-\nu-2}{2}} \binom{p-\nu}{2j+1}(3b)^{2j}a^{p-\nu-2-2j}, \tag{5.11}$$

where, in our case, $\nu = 1$ or $\nu = 3$. We also recall that

$$a^2 + 3b^2 = p. \tag{5.12}$$

First we show that $(a+3b)^{p-1} - (a-3b)^{p-1}$ is divisible by p, provided that (5.12) holds. To do this, we use properties of the well-known Chebyshev polynomials of the second kind, $U_n(x)$, which can be written as

$$U_n(x) = \frac{(x+\sqrt{x^2-1})^{n+1} - (x-\sqrt{x^2-1})^{n+1}}{2\sqrt{x^2-1}}; \tag{5.13}$$

see, e.g., [18, p. 10]. Using the substitution

$$x = \frac{a}{\sqrt{a^2-9b^2}} \tag{5.14}$$

we see that

$$(a+3b)^{p-1} - (a-3b)^{p-1} = 6b\left(\sqrt{a^2-9b^2}\right)^{p-2} U_{p-2}(x). \tag{5.15}$$

On the other hand, it is known (see, e.g., Exercise 1.2.15(e) in [18, p. 9]) that a Chebyshev polynomial of the form $U_{6k-1}(x)$, which is the case here, is always divisible by $U_2(x) = 4x^2 - 1$. Now, in our case we have, with (5.14),

$$4x^2 - 1 = \frac{3}{a^2-9b^2}(a^2+3b^2),$$

which means that $(a+3b)^{p-1} - (a-3b)^{p-1}$ is indeed divisible by $a^2 + 3b^2$. Hence (5.10) follows if we can show that

$$\frac{(a+3b)^{p-1} - (a-3b)^{p-1}}{a^2+3b^2} + (a+3b)^{p-3} - (a-3b)^{p-3} \equiv 0 \pmod{p}. \tag{5.16}$$

We begin with the second half of the left-hand side and note that by Fermat's little theorem we have

$$(a+3b)^{p-3} - (a-3b)^{p-3} \equiv \frac{1}{(a+3b)^2} - \frac{1}{(a-3b)^2} = \frac{-12ab}{(a^2-9b^2)^2} \pmod{p}. \tag{5.17}$$

To deal with the first part of (5.16), we rewrite as a formal power series

$$\frac{1}{a^2+3b^2}=\frac{1}{a^2}\cdot\frac{1}{1+3\frac{b^2}{a^2}}=\frac{1}{a^2}\sum_{j=0}^{\infty}(-1)^j3^j\frac{b^{2j}}{a^{2j}}, \tag{5.18}$$

and take the Cauchy product with the sum on the right of (5.11), with $\nu=1$:

$$\begin{aligned}\left(\sum_{j=0}^{\frac{p-3}{2}}\binom{p-1}{2j+1}(3b)^{2j}a^{p-3-2j}\right)&\left(\sum_{j=0}^{\infty}(-1)^j3^j\frac{b^{2j}}{a^{2j}}\right)\\&=\sum_{n=0}^{\frac{p-3}{2}}\left(\sum_{j=0}^{n}\binom{p-1}{2j+1}(-3)^j\right)(-3)^nb^{2n}a^{p-3-2n}.\end{aligned} \tag{5.19}$$

(Note that the right-hand sum over n must be finite by the divisibility property we proved above. In fact, the term for $n=(p-3)/2$ must vanish because of (5.18); see the remark following the proof). Using the simple congruence

$$\binom{p-1}{2j+1}=\frac{(p-1)(p-2)\cdots(p-(2j+1))}{1\cdot2\cdots(2j+1)}\equiv(-1)^{2j+1}=-1\pmod{p},$$

we evaluate the inner sum of (5.19) as

$$\sum_{j=0}^{n}\binom{p-1}{2j+1}(-3)^j\equiv\frac{(-3)^{n+1}-1}{4}\pmod{p}, \tag{5.20}$$

and so the right-hand side of (5.19) becomes

$$\sum_{n=0}^{\frac{p-3}{2}}\frac{(-3)^{n+1}-1}{4}(-3)^nb^{2n}a^{p-3-2n}=\frac{-a^{p-3}}{4}\left(3\sum_{n=0}^{\frac{p-3}{2}}\left(\frac{3^2b^2}{a^2}\right)^n+\sum_{n=0}^{\frac{p-3}{2}}\left(\frac{-3b^2}{a^2}\right)^n\right).$$

Now from (5.12) we get

$$\frac{-3b^2}{a^2}=1-\frac{p}{a^2}\equiv1\pmod{p},$$

and therefore the second summation in the previous line is congruent to $\frac{p-1}{2}\equiv\frac{-1}{2}$ (mod p). The first summation is

$$\frac{\left(\frac{3^2b^2}{a^2}\right)^{(p-1)/2}-1}{\frac{3^2b^2}{a^2}-1}\equiv0\pmod{p},$$

by Fermat's little theorem. Hence the right-hand side of (5.19) is congruent to

$$-\frac{1}{4}a^{p-3}\cdot\frac{-1}{2}\equiv\frac{1}{8a^2}\pmod{p},$$

where we have used Fermat's little theorem again. Thus, with (5.11), (5.18) and (5.19) we get

$$\frac{(a+3b)^{p-1}-(a-3b)^{p-1}}{a^2+3b^2}\equiv6ab\cdot\frac{1}{a^2}\cdot\frac{1}{8a^2}\equiv\frac{3b}{4a^3}\pmod{p}. \tag{5.21}$$

Finally, combining (5.21) with (5.17) we see that the left-hand side of (5.16) is congruent to

$$\begin{aligned}\frac{3b}{4a^3}-\frac{12ab}{(a^2-9b^2)^2}&=3b\frac{81b^4-18b^2a^2-15a^4}{a^3(a^2-9b^2)^2}\\&=-9b\frac{(a^2+3b^2)(5a^2-9b^2)}{a^3(a^2-9b^2)^2}\equiv 0 \pmod{p},\end{aligned}$$

by (5.12). This proves the congruence (5.16) and thus completes the proof of Lemma 5. □

Remark: The fact that the term for $n=(p-3)/2$ in (5.19) vanishes modulo p, can also be verified using quadratic reciprocity. Indeed, from (5.19) we see that this term is $\frac{1}{4}((-3)^{(p-1)/2}-1) \pmod{p}$. But by Euler's criterion we have

$$(-3)^{\frac{p-1}{2}}\equiv\left(\frac{-3}{p}\right)=1 \pmod{p},$$

where the evaluation of the Legendre symbol as 1 for all primes $p\equiv 1 \pmod{6}$ follows easily from quadratic reciprocity. Hence the sum in question is $0 \pmod{p}$.

6. Primes satisfying $p^2=3x^3+3x+1$

In this final section we study primes p that satisfy the property that $p^2=3x^3+3x+1$ for some integer x. The main result will be the fact that all these primes are "exceptional" for $M=3$, in the sense of Section 4 and Table 3. We begin with another result that is interesting in its own right and is related to the basic question of this paper, namely the orders of certain Gauss factorials.

Proposition 6.1. *Let p be a prime such that $p^2=3x^2+3x+1$ for some integer x. Then*

$$\text{ord}_p(\frac{p-1}{3}!)=\begin{cases}36 & \textit{for} \quad p\neq 13,\\ 12 & \textit{for} \quad p=13.\end{cases} \tag{6.1}$$

This is then used at the end of the section to prove

Proposition 6.2. *Every prime p that satisfies $p^2=3x^2+3x+1$ for some integer x is an exceptional prime for $M=3$, i.e., we have $\gamma_1^{(3)}=\gamma_2^{(3)}$.*

The same two results also hold for $M=6$:

Proposition 6.3. *Let p be a prime such that $p^2=3x^2+3x+1$ for some integer x. Then*

$$\text{ord}_p(\frac{p-1}{6}!)=\begin{cases}36 & \textit{for} \quad p\neq 13,\\ 12 & \textit{for} \quad p=13.\end{cases}$$

This, together with Proposition 5.1, immediately gives the following

Corollary 4. *Every prime p that satisfies $p^2=3x^2+3x+1$ for some integer x is an exceptional prime for $M=6$, i.e., we have $\gamma_1^{(6)}=\gamma_2^{(6)}$.*

Remarks: (1) Primes that satisfy $p^2=3x^2+3x+1$ are necessarily of the form $p\equiv 1 \pmod{6}$. Indeed, if we rewrite the equation as $12p^2=(6x+3)^2+3$, we see that -3 is a quadratic residue modulo p, which is the case if and only if $p\equiv 1$

(mod 6), as we already remarked at the end of Section 5. But see also Corollary 5 below.

(2) The converse of Proposition 6.2 is not true: $p = 76\,543$ is an exceptional prime (see Table 3) but does not satisfy $p^2 = 3x^2 + 3x + 1$. In fact, $\mathrm{ord}_p(\frac{p-1}{3}!) = 12\,757 = \frac{p-1}{6}$. This is the only such case up to $4 \cdot 10^8$.

(3) In view of Propositions 6.1 and 6.3 it must be pointed out that in general we do *not* have $\mathrm{ord}_p(\frac{p-1}{3}!) = \mathrm{ord}_p(\frac{p-1}{6}!)$. Indeed, already the smallest relevant prime, $p = 7$, shows that $\mathrm{ord}_7 2 = 3 \neq \mathrm{ord}_7 1 = 1$.

All the proofs in this section rely in an essential way on the easy observation that the equation $p^2 = 3x^2 + 3x + 1$ can be rewritten in the form of the Pell equation

$$(2p)^2 - 3(2x+1)^2 = 1. \tag{6.2}$$

The infinitely many solutions (A_n, B_n) of the equation

$$A^2 - 3B^2 = 1 \tag{6.3}$$

are given by the recurrence relations (see, e.g., [16, p. 354])

$$A_{n+1} = 2A_n + 3B_n, \qquad B_{n+1} = A_n + 2B_n, \tag{6.4}$$

with initial conditions $A_1 = 2$, $B_1 = 1$. Combining these two identities, we immediately get

$$A_{n+2} = 4A_{n+1} - A_n, \qquad A_0 = 1, A_1 = 2, \tag{6.5}$$

$$B_{n+2} = 4B_{n+1} - B_n, \qquad B_0 = 0, B_1 = 1. \tag{6.6}$$

With standard methods using the characteristic equation $x^2 - 4x + 1 = 0$ and its roots $2 \pm \sqrt{3}$, we get the explicit formulas

$$A_n = \frac{1}{2}\left((2+\sqrt{3})^n + (2-\sqrt{3})^n\right), \tag{6.7}$$

$$B_n = \frac{1}{2\sqrt{3}}\left((2+\sqrt{3})^n - (2-\sqrt{3})^n\right). \tag{6.8}$$

The first few values of A_n and B_n are shown in Table 4.

n	0	1	2	3	4	5	6	7	8	9	10
A_n	1	2	7	26	97	362	1 351	5 042	18 817	70 226	262 087
B_n	0	1	4	15	56	209	780	2 911	10 864	40 545	151 316

Table 4: A_n, B_n for $0 \leq n \leq 10$.

It is also worth mentioning that the quotients A_n/B_n are approximants to $\sqrt{3}$. In what follows we need a number of properties of the sequences $\{A_n\}$ and $\{B_n\}$. While they could be obtained directly from (6.5)–(6.8), it is convenient to use the close relationships with the Chebyshev polynomials, $T_n(x)$ and $U_n(x)$, of the first and second kind, respectively. By comparing (6.7) with the well-known explicit expansion

$$T_n(x) = \frac{1}{2}\left((x+\sqrt{x^2-1})^n + (x-\sqrt{x^2-1})^n\right),$$

and comparing (6.8) with (5.13), we immediately get

$$A_n = T_n(2), \qquad B_n = U_{n-1}(2); \tag{6.9}$$

see also the entries A001075 and A001353 in [19]. Using the identities (22.7.24) and (22.7.25) in [1, p. 782] along with (6.9), we obtain the two complementary identities (for $n \geq m$)

$$2A_mA_n = A_{m+n} + A_{n-m}, \tag{6.10}$$

$$6B_mB_n = A_{m+n} - A_{n-m}. \tag{6.11}$$

We also have the identity

$$A_{n-2}A_n - A_{n-1}^2 = 3, \tag{6.12}$$

which can be obtained by first setting $m = n-2$ in (6.10), and then taking (6.10) with n replaced by $n-1$ and setting $m = n-1$, and finally subtracting the two identities thus obtained.

The following parity and congruence properties can be observed in Table 4 and are easy to prove:

Lemma 6. *For all $k \geq 0$ we have*

$$A_{2k+1} \text{ and } B_{2k} \text{ are even, } A_{2k} \text{ and } B_{2k+1} \text{ are odd,} \tag{6.13}$$

$$A_k \equiv (-1)^k \pmod 3, \tag{6.14}$$

$$B_{3k} \equiv 0 \pmod 3, \qquad B_{3k+1} \equiv B_{3k+2} \equiv (-1)^k \pmod 3. \tag{6.15}$$

Proof. From (6.5) we get $A_{n+2} \equiv A_n \pmod 2$ and $A_{n+2} \equiv A_{n+1} - A_n \pmod 3$, and similarly for B_n. The results now follow by easy inductions. □

We now return from the general case to the specific situation given by (6.2). By (6.13), the term $2p$ can correspond only to an odd-index term A_n; so for a given prime p satisfying $p^2 = 3x^2 + 3x + 1$ we have, for some k,

$$p = \frac{1}{2}A_{2k-1}, \qquad x = \frac{1}{2}\left(B_{2k-1} - 1\right). \tag{6.16}$$

The first few primes of this type are shown in Table 5.

$2k-1$	p	r	s
3	13	(-5)	(3)
5	181	7	15
7	2 521	97	15
11	489 061	-362	780
13	6 811 741	-5 042	780
17	1 321 442 641	18 817	40 545
19	18 405 321 661	262 087	40 545

Table 5: Primes $p = \frac{1}{2}A_{2k-1}$, $2k-1 \leq 19$, and $4p = r^2 + 3s^2$.

Table 5 might give the impression that p is prime if and only if $2k-1$ is prime, but this is far from true: the next values of $2k-1$ for which $\frac{1}{2}A_{2k-1}$ is prime are 79, 151, 199, 233, 251, 317, 816, and 971; these are all with $2k-1 < 1000$. However, we have the following

Lemma 7. *If $p = \frac{1}{2}A_{2k-1}$ is prime then $2k-1$ is prime.*

Proof. It is known (see [18, p. 228], Remark 2) that for $k \geq 2$ the polynomial $\frac{1}{x}T_{2k-1}(x)$ is irreducible over $\mathbb{Q}$ if and only if $2k-1$ is prime. With (6.9) this basically proves the result, but we still have to show that the linear factors $x-1$ and $x-3$ cannot occur when $\frac{1}{x}T_{2k-1}(x)$ is reducible (since they would only result in the units ± 1). However, the polynomials $T_n(x)$ have the well-known complete factorization (see, e.g., [18, p. 10])

$$T_n(x) = 2^{n-1}\prod_{j=1}^{n}\left(x - \cos\tfrac{(2j-1)\pi}{2n}\right),$$

and it is clear that the cosine terms cannot be 1 or 3. □

In Remark (2) following Proposition 6.2 we showed that necessarily $p \equiv 1 \pmod 6$. Proposition 6.1 actually implies more. Since for $p \neq 13$ the order in question is 36, $p-1$ must be divisible by 36. But also, in Table 5 we see that these primes all end in 1, which of course indicates a congruence modulo 5. In fact, we have the following result which we are going to prove independently of Proposition 6.1.

Corollary 5. *Let $p \neq 13$ be a prime that satisfies $p^2 = 3x^2 + 3x + 1$. Then $p \equiv 1 \pmod{180}$.*

Proof. By (6.16) we need to consider the terms $\frac{1}{2}A_{2k-1}$. With an easy manipulation of the recurrence (6.5) we obtain the relation $A_{n+2} = 14A_n - A_{n-2}$, and using this we can show with a straightforward induction that

$$\frac{1}{2}A_{2k-1} \equiv \begin{cases} 1 \pmod{36} \quad\text{and}\quad 1 \pmod 5 & \text{for}\quad 2k+1 \not\equiv 0 \pmod 3,\\ 13 \pmod{36} \quad\text{and}\quad 3 \pmod 5 & \text{for}\quad 2k+1 \equiv 0 \pmod 3.\end{cases}$$

However, by Lemma 7 we have $2k+1 \not\equiv 0 \pmod 3$ unless $2k+1 = 3$ (the case $p = 13$). Thus, for any other prime of the given form we have, by the Chinese remainder theorem, $p = \frac{1}{2}A_{2k-1} \equiv 1 \pmod{5\cdot 36}$, as required. □

Next we need the following identities.

Lemma 8. *Let $p = \frac{1}{2}A_{2k-1}$ be a prime. Then*

$$4p = A_{k-1}^2 + 3B_k^2 = A_k^2 + 3B_{k-1}^2. \tag{6.17}$$

Proof. For the first identity, we set $n = m = k-1$ in (6.10) and $n = m = k$ in (6.11). Then we add both equations and obtain

$$2A_{k-1}^2 + 6B_k^2 = A_{2k-2} + A_{2k} = 4A_{2k-1} = 8p,$$

where the middle equality follows from (6.5). Finally, we divide both sides by 2. The second part of (6.17) is obtained analogously. □

A key ingredient in the proof of Proposition 6.1 is the theorem of Jacobi, namely the modulo p version of (5.6):

$$\binom{\frac{2p-2}{3}}{\frac{p-1}{3}} \equiv -r \pmod p, \tag{6.18}$$

where

$$4p = r^2 + 3s^2, \qquad r \equiv 1 \pmod 3, \quad s \equiv 0 \pmod 3. \tag{6.19}$$

Now it is easy to connect (6.19) with (6.17):

Lemma 9. *Let* $p = \frac{1}{2}A_{2k-1}$ *be a prime.*

(a) *If* $2k-1 \equiv 1 \pmod{3}$ *then* $r = (-1)^k A_k$ *and* $4p = A_k^2 + 3B_{k-1}^2$.

(b) *If* $2k-1 \equiv -1 \pmod{3}$ *then* $r = (-1)^{k-1} A_{k-1}$ *and* $4p = A_{k-1}^2 + 3B_k^2$.

Proof. Lemma 8 gives two different representations; we have to choose the one that satisfies the conditions in (6.19).

(a) If $2k-1 \equiv 1 \pmod{3}$ then $k \equiv 1 \pmod{3}$ and so, by (6.15), $B_{k-1} \equiv 0 \pmod{3}$, as required. Furthermore, by (6.14) we have $(-1)^k A_k \equiv 1 \pmod{3}$, and this proves part (a).

(b) Similarly, if $2k-1 \equiv -1 \pmod{3}$ then $k \equiv 0 \pmod{3}$ and so $B_k \equiv 0 \pmod{3}$. Also, $(-1)^{k-1}A_{k-1} \equiv 1 \pmod{3}$, which proves part (b). □

The last two columns of Table 5 may serve to illustrate Lemma 9; see also Table 4. Although $p = 13$ is of the form $\frac{1}{2}A_{2k-1}$, it is not covered by Lemma 9 and the values of r and s do not come from either of the representations in (6.17).

We are now in a position to prove Propositions 6.1 and 6.2.

Proof of Proposition 6.1. With the aim of using Jacobi's theorem (6.18), we rewrite

$$\frac{2p-2}{3}! = \frac{(p-1)!}{(p-1)(p-2)\cdots(p-\frac{p-1}{3})} \equiv \frac{-1}{\frac{p-1}{3}!} \pmod{p}, \tag{6.20}$$

where in the numerator we have used Wilson's theorem (1.1), and in the denominator the fact that $(p-1)/3$ is even. With (6.18) we therefore get

$$\left(\frac{p-1}{3}!\right)^3 \equiv \frac{1}{r} \pmod{p}. \tag{6.21}$$

In the exceptional case $p = 13$ we have $r^2 = (-5)^2 \equiv -1 \pmod{13}$ (see Table 5), which verifies (6.1) in this case. We now assume that $p \neq 13$ and first consider the case $2k-1 \equiv 1 \pmod{3}$.

By Lemma 9(a) and (6.10) with $m = n = k$ we have

$$r^2 = A_k^2 = \frac{1}{2}\left(A_{2k}+1\right). \tag{6.22}$$

Squaring this and using the fact that by (6.12) we have

$$A_{2k}^2 = A_{2k-1}A_{2k} - 3 \equiv -3 \pmod{p}, \tag{6.23}$$

we then obtain

$$r^4 = \frac{1}{4}\left(A_{2k}^2 + 2A_{2k} + 1\right) \equiv \frac{1}{2}\left(A_{2k} - 1\right) \pmod{p}. \tag{6.24}$$

Finally, upon multiplying the congruences (6.22) and (6.24), we get

$$r^6 = r^2 \cdot r^4 \equiv \frac{1}{4}\left(A_{2k}^2 - 1\right) \equiv \frac{1}{4}(-3-1) = -1 \pmod{p},$$

where we have used (6.23) again.

It remains to show that we cannot have $r^4 \equiv 1 \pmod{p}$. If this were the case then by (6.24) we would have $A_{2k} \equiv 3 \pmod{p}$, and thus $A_{2k}^2 \equiv 9 \pmod{p}$. However, by (6.23) we know that $A_{2k}^2 \equiv -3 \pmod{p}$. This is a contradiction for any prime $p > 3$.

The case $2k-1 \equiv -1 \pmod{3}$ can be treated analogously, with $r^2 = A_{k-1}^2$ by Lemma 9(b). Altogether we have shown that $r^{12} \equiv 1 \pmod{p}$, with no smaller power being $\equiv 1 \pmod p$. This, with (6.21), completes the proof of Proposition 6.1. □

Proof of Proposition 6.2. We need to show that

$$\operatorname{ord}_{p^2}\left(\left(\tfrac{p^2-1}{3}\right)_p!\right) = \begin{cases} 36 & \text{for} \quad p \neq 13, \\ 12 & \text{for} \quad p = 13. \end{cases} \tag{6.25}$$

We proceed in a similar fashion as in the proof of Proposition 6.1, but instead of Jacobi's theorem we use the generalization

$$\frac{\left(\tfrac{2(p^2-1)}{3}\right)_p!}{\left(\left(\tfrac{p^2-1}{3}\right)_p!\right)^2} \equiv -r + \frac{p}{r} \pmod{p^2}, \tag{6.26}$$

which is a special case of Theorem 8 in [7]. In analogy to (6.20) we note that

$$\left(\frac{2(p^2-1)}{3}\right)_p! \left(\frac{p^2-1}{3}\right)_p! \equiv (p^2-1)_p! \equiv -1 \pmod p,$$

where the right-most congruence follows from the Gauss-Wilson theorem (1.4). With (6.26) we now have

$$\left(\left(\frac{p^2-1}{3}\right)_p!\right)^{-3} \equiv r - \frac{p}{r} \pmod{p^2}. \tag{6.27}$$

First we consider $p = 13$. Then, since $r = -5$, we have

$$\left(-5 + \frac{13}{5}\right)^2 \equiv 25 - 2 \cdot 13 = -1 \pmod{13^2},$$

so the order in this case is 12.

Now suppose that $2k-1 \equiv 1 \pmod 3$; then, as before, $r^2 = A_k^2$. With $2p = A_{2k-1}$, as before, we have

$$\left(r - \frac{p}{r}\right)^2 \equiv r^2 - 2p = A_k^2 - A_{2k-1} \pmod{p^2}.$$

We denote, for a moment, the right-most term by X_k. We need to show that $X_k^3 \equiv -1 \pmod{p^2}$. But since

$$X_k^3 + 1 = (X_k + 1)(X_k^2 - X_k + 1)$$

and $X_k \not\equiv -1 \pmod p$ by Proposition 6.1, we are done if we can show that $X_k^2 - X_k + 1 \equiv 0 \pmod{p^2}$. But

$$\begin{aligned} X_k^2 - X_k + 1 &= A_k^4 - 2A_k^2 A_{2k-1} + A_{2k-1}^2 - A_k^2 + A_{2k-1} + 1 \\ &\equiv A_k^4 - A_k^2 + 1 + A_{2k-1}(1 - 2A_k^2) \pmod{p^2} \\ &= (A_k^2 - \tfrac{1}{2})^2 + \tfrac{3}{4} - A_{2k-1}A_{2k} = \tfrac{1}{4}A_{2k}^2 + \tfrac{3}{4} - A_{2k-1}A_{2k} \\ &= \tfrac{1}{4}A_{2k-1}A_{2k+1} - A_{2k-1}A_{2k} = -\tfrac{1}{4}A_{2k-1}^2 \equiv 0 \pmod{p^2}, \end{aligned}$$

where we have used (6.22), (6.12), and (6.5). This proves (6.25) in the case $2k-1 \equiv 1 \pmod 3$. The case $2k-1 \equiv -1 \pmod 3$ is completely analogous. □

Proof of Proposition 6.3 (sketch). For the sake of brevity we only mention that we use the mod p version of (5.5) together with the congruence $r^3 \equiv u^3 \pmod{p}$, which is an easy consequence of (5.4). The result then follows from Proposition 6.1. We leave the details to the reader. □

Remarks: (1) Since this section concerns primes satisfying $p^2 = 3x^2 + 3x + 1$, it is worth mentioning here that primes of the form $p = 3x^2 + 3x + 1$ are also of considerable interest in connection with orders of Gauss factorials. In fact, it can be shown that for a prime $p \equiv 1 \pmod{3}$, the factorial $\frac{p-1}{3}!$ has order 1, 3, or 9 modulo p if and only if $p = 3x^2 + 3x + 1$ for some integer x. This, and related results, will be part of a forthcoming paper [8] by the authors.

(2) One may now wonder what can be said about primes p satisfying $p^n = 3x^2 + 3x + 1$ for $n \geq 3$. First, since we can rewrite this as $p^n = (x+1)^3 - x^3$, it follows from Fermat's last theorem for the exponent 3 that there can be no solution when $n \equiv 0 \pmod{3}$. For all other $n > 3$, this is an instance of the "Generalized Fermat Conjecture" (see [10] for a survey) which would imply that there are no solutions. It follows from proven results that there are at most finitely many integer solutions.

Furthermore, it should be mentioned that in the cases $n = 1$ and $n = 2$ one does not know whether there are infinitely many primes satisfying each of these two equations, although this has been conjectured in more general situations. See [12], Sections A1 and A3, for more information and references.

(3) The sequence $\{B_n\}$ of (6.4) and (6.6) also occurs in connection with the case $M = 4$: It can be shown that a prime $p \equiv 1 \pmod{4}$ satisfies $\big((p-1)/4\big)!^8 \equiv -1 \pmod{p}$ if and only if $p = B_k^2 + B_{k+1}^2$; this will also be part of a forthcoming paper [8] by the authors. See also [4, p. 316 ff.] for a brief account of this.

Acknowledgment

We would like to thank Yves Gallot who generously tailor-made a very fast program for us, enabling a search for $M = 3$ and 4 exceptional primes, and also for primes $p \equiv 1 \pmod{4}$ satisfying $w_p + 2q_p(2) \equiv 0 \pmod{p}$.

References

[1] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions.* National Bureau of Standards, 1964.

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

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

[4] J. M. Borwein and D. Bailey, *Mathematics by experiment. Plausible reasoning in the 21st Century.* Second edition. A K Peters, Ltd., Wellesley, MA, 2008.

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

[6] J. B. Cosgrave and K. Dilcher, *Extensions of the Gauss-Wilson theorem*, Integers **8**, A39, 15 pp.

[7] J. B. Cosgrave and K. Dilcher, *Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients*, preprint, 2009.

[8] J. B. Cosgrave and K. Dilcher, *The Gauss-Wilson theorem for one-third and one-quarter intervals*, in preparation.

[9] R. E. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433–449.

[10] H. Darmon, *Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation*, C. R. Math. Rep. Acad. Sci. Canada **19** (1997), no. 1, 3–14, 64.

[11] L. E. Dickson, *History of the Theory of Numbers. Volume I: Divisibility and Primality*. Chelsea Publishing Company, 1971.

[12] R. K. Guy, *Unsolved problems in number theory*. Third edition. Problem Books in Mathematics. Springer-Verlag, New York, 2004.

[13] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. Oxford Ser. **39** (1938), 350–360.

[14] Maple, `http://www.maplesoft.com/`.

[15] L. J. Mordell, *The congruence* $(p-1/2)! \equiv \pm 1 \pmod{p}$, Amer. Math. Monthly **68** (1961), 145–146.

[16] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*. 5th ed., Wiley, 1991.

[17] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*. Springer-Verlag, New York, 1979.

[18] T. J. Rivlin, *Chebyshev Polynomials*. Second edition, Wiley, New York, 1990.

[19] N. J. A. Sloane, *On-Line Encyclopedia of Integer Sequences*. `http//www.research.att.com/~njas/sequences/`.

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

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada
E-mail address: `dilcher@mathstat.dal.ca`