Functiones et Approximatio
54.1 (2016), 73–93
doi: 10.7169/facm/2016.54.1.7

THE MULTIPLICATIVE ORDERS OF CERTAIN GAUSS FACTORIALS, II

John B. Cosgrave, Karl Dilcher

Abstract: We study the multiplicative orders of $\left(\frac{n-1}{M}\right)_n!$ (mod n) for odd prime powers $n = p^\alpha$, $p \equiv 1 \pmod{M}$, where the Gauss factorial $N_n!$ denotes the product of all integers up to N that are relatively prime to n. Departing from previously obtained results on the connection between the order for p^α and for $p^{\alpha+1}$, we obtain new criteria for exceptions to a general pattern, with particular emphasis on the cases $M = 3$, $M = 4$ and $M = 6$. In the process we also obtain some results of independent interest. Most results are based on generalizations of binomial coefficient congruences of Gauss, Jacobi, and Hudson and Williams.

Keywords: Gauss-Wilson theorem, factorials, Gauss factorials, binomial coefficient congruences.

1. Introduction

The factorial-like product of integers,

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

defined for positive integers N and n, plays an important role in number theory, for instance in the definition of Morita's p-adic Gamma function (see, e.g., [1, p. 277]). We call this product a *Gauss factorial*, a terminology suggested by the *Gauss-Wilson theorem* which states that for any integer $n \geqslant 2$ we have

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

where p is an odd prime and α is a positive integer. In the previous papers [2], [4], and [5] we studied the Gauss factorials $(\frac{n-1}{M})_n!$, $M \geqslant 1$, $n \equiv 1 \pmod{M}$. For

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

2010 Mathematics Subject Classification: primary: 11A07; secondary: 11B65

$M = 1$ this is just the Gauss-Wilson theorem (1.2), and the case $M = 2$ and p prime was first considered by Lagrange in 1773 (see [8, p. 275]). Later Mordell [13] completely determined the multiplicative orders (modulo p), and the present authors [2] extended this to arbitrary positive integers n. While much can be said about the case of general $M \geqslant 2$ and n having two or more distinct prime factors congruent to 1 modulo M (see [5] and [6]), a particularly interesting and challenging case occurs when $n = p^\alpha$, $p \equiv 1 \pmod{M}$. In fact, it is the purpose of this paper to continue our study in [4] of the multiplicative orders of

$$\left(\tfrac{p^\alpha-1}{M}\right)_{p^\alpha}! \pmod{p^\alpha}, \qquad p \equiv 1 \pmod{M}, \qquad M \geqslant 2. \tag{1.3}$$

While everything is known when $M = 2$, and a number of results for general M were obtained in [4], this paper will be mainly devoted to the cases $M = 3, 4$, and 6. This is not because they are "next in line", but rather, the theory of Jacobi sums makes it possible to obtain particular results, and explain special phenomena, that do not apparently occur in other cases.

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

$$\gamma_\alpha^M(p) := \operatorname{ord}_{p^\alpha}\left(\left(\tfrac{p^\alpha-1}{M}\right)_{p^\alpha}!\right) \tag{1.4}$$

for varying integers $\alpha \geqslant 1$. Clearly $(\frac{p^\alpha-1}{M})_{p^\alpha}! = (\frac{p^\alpha-1}{M})_p!$; in what follows we will therefore replace the subscript p^α in the Gauss factorial by p.

Since the case $M = 2$ is completely determined, we consider mainly $M \geqslant 3$. We illustrate the sequence of orders for $\alpha = 1, 2, \ldots$ with two examples for $M = 3$.

Example 1. When $p = 7$, we have $\frac{p-1}{3} = 2$ and the Gauss factorial is just the ordinary factorial, namely 2. We immediately see that $\gamma_1^3(7) = 3$. Using computer algebra, we furthermore find $\gamma_2^3(7) = 21$, $\gamma_3^3(7) = 147$, and writing $\gamma := \gamma_1^3(7)$, it appears that we obtain the sequence $\gamma, \gamma p, \gamma p^2, \gamma p^3, \ldots$

Example 2. When $p = 13$, we have $\frac{p-1}{3} = 4$ and once again the Gauss factorial is the ordinary factorial, $4! \equiv 11 \pmod{13}$. It is now easy to verify that $\gamma_1^3(13) = 12$. Furthermore, computer algebra yields $\gamma_2^3(13) = 12$ also, while we get $\gamma_3^3(13) = 12 \cdot 13$, and it appears that in this case the sequence $\{\gamma_\alpha^M(p)\}$, $\alpha = 1, 2, \ldots$, is of the form $\gamma, \gamma, \gamma p, \gamma p^2, \ldots$, in contrast to the first example.

These two examples are special cases of one of the main results in [4], namely Proposition 2.2, which relates the order $\gamma_{\alpha+1}^M(p)$ with $\gamma_\alpha^M(p)$, for $\alpha \geqslant 1$:

Theorem 1 ([4]). *Let $M \geqslant 2$ be an integer, let $p \equiv 1 \pmod{M}$ be a prime, and for $\alpha \geqslant 1$ let $\gamma_\alpha^M(p)$ be defined as in* (1.4). *If $p \equiv 1 \pmod{2M}$, then*

$$\gamma_{\alpha+1}^M(p) = p\gamma_\alpha^M(p) \qquad \text{or} \qquad \gamma_{\alpha+1}^M(p) = \gamma_\alpha^M(p). \tag{1.5}$$

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

$$\gamma_{\alpha+1}^M(p) = \begin{cases} p\gamma_\alpha^M(p) \quad \text{or} \quad \gamma_\alpha^M(p) & \text{when} \quad \gamma_\alpha^M(p) \equiv 0 \pmod 4, \\ \frac{1}{2}p\gamma_\alpha^M(p) \quad \text{or} \quad \frac{1}{2}\gamma_\alpha^M(p) & \text{when} \quad \gamma_\alpha^M(p) \equiv 2 \pmod 4, \\ 2p\gamma_\alpha^M(p) \quad \text{or} \quad 2\gamma_\alpha^M(p) & \text{when} \quad \gamma_\alpha^M(p) \equiv 1 \pmod 2. \end{cases} \tag{1.6}$$

Numerical experiments show that almost always the first alternative in the various cases in Theorem 1 holds, with very few exceptions such as the case of Example 2. For the sake of completeness we display an excerpt of Table 3 in [4] as Table 1 below.

Table 1: Exceptional ($\alpha = 1$) primes $p < 2 \cdot 10^6$ for $3 \leqslant M \leqslant 10$.

M	p
3	13, 181, 2 521, 76 543, 489 061
4	29 789
5	71
6	13, 181, 2 521, 76 543, 489 061
10	11

All these exceptional primes occur at $\alpha = 1$. We have not found any for $\alpha \geqslant 2$, and will return to this point in the next section. It was a major part of [4], and will also be so in the present paper, to establish criteria and characterizations for the exceptionality of these primes. While this paper will be mainly devoted to the special cases $M = 3$, 4 and 6, we begin by quoting a general criterion from [4]. We first need some definitions.

For any prime p, the *Wilson quotient* is defined by

$$w(p) := \frac{(p-1)! + 1}{p}. \tag{1.7}$$

By Wilson's theorem, $w(p)$ is obviously an integer; often the Wilson quotient is considered modulo p. Next, for any positive integer $M \geqslant 2$ and prime $p \equiv 1 \pmod{M}$ we define the sum

$$S^M(p) := \sum_{j=1}^{\frac{p-1}{M}} \frac{1}{j}. \tag{1.8}$$

For $M = 2$, 3, 4 and 6 there are well-known evaluations of such sums modulo p in terms of Fermat quotients; see, e.g., [12] or [3]. Finally, for given $\alpha \geqslant 1$, $M \geqslant 2$ and $p \equiv 1 \pmod{M}$ we define $V_\alpha^M(p)$ by

$$\left(\left(\frac{p^\alpha - 1}{M} \right)_p ! \right)^{\gamma_\alpha^M(p)} \equiv 1 + V_\alpha^M(p) p^\alpha \pmod{p^{\alpha+1}}, \tag{1.9}$$

where $\gamma_\alpha^M(p)$ is the order defined in (1.4). We are now ready to state the following supplementary result to Theorem 1, which can be found as the final part of Proposition 4.2 in [4].

Theorem 2. *With M, p and α as in Theorem 1, the first alternative in each case of* (1.5), (1.6) *holds if and only if*

$$T_\alpha^M(p) := V_\alpha^M(p) + \tfrac{1}{M} \gamma_\alpha^M(p) \left(w(p) - S^M(p) \right) \not\equiv 0 \pmod{p}. \tag{1.10}$$

While it is not our intention to repeat the proof of this result and of Theorem 1, we would like to put the expression $T_\alpha^M(p)$ into perspective. Let us take, for instance, $M = 3$. Then by definition of the order we obviously have, for a given $\alpha \geqslant 1$,

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

Much less obvious is the congruence

$$\left(\left(\tfrac{p^{\alpha+1}-1}{3}\right)_p!\right)^{\gamma_\alpha^3(p)} \equiv 1 + T_\alpha^3(p)p^\alpha \pmod{p^{\alpha+1}}; \tag{1.11}$$

the general case of this lies at the heart of the proof of both Theorems 1 and 2. Indeed, the congruence (1.11) shows that in the case when $T_\alpha^3(p) \equiv 0 \pmod{p}$, by the definition (1.4) we have $\gamma_{\alpha+1}^3(p) = \gamma_\alpha^3(p)$. On the other hand, when $T_\alpha^3(p) \not\equiv 0 \pmod{p}$, we raise both sides of the congruence (1.11) to the power p, and we see that in this case $\gamma_{\alpha+1}^3(p) = p\gamma_\alpha^3(p)$. All this, of course, is consistent with Theorems 1 and 2.

The condition (1.10) was used to find the entries in Table 1 for all $p < 2 \cdot 10^6$, using the computer algebra system Maple. In the cases $M = 3$, 4 and 6, aided by the connection between the sums $S^M(p)$ and Fermat quotients, we were able to extend the computations to $p < 10^8$; this was later extended at our request by Yves Gallot [9] to $4 \cdot 10^8$. On the other hand, due to the obvious difficulty of computing $V_\alpha^M(p)$ for $\alpha = 2$, we were able to search for "$\alpha = 2$ exceptional primes" only for $p < 10^4$, without finding any. See, however, the remarks following Theorem 3 below.

The above results, quoted from [4], may serve as motivation for the new results in the present paper. In particular, in the cases $M = 3$, 4 and 6 we will

– give a new and much faster test for exceptional primes, which will also lead to some new theoretical results;

– further investigate the coincidence of exceptional primes for $M = 3$ and $M = 6$.

However, we begin with a matter that is related to Theorem 1 and Example 2.

2. Descending exceptionality

Considering Examples 1 and 2 with $M = 3$, it is conceivable that there exists a prime $p \equiv 1 \pmod 3$ such that $\gamma_1^3(p) = \gamma$, $\gamma_2^3(p) = p\gamma$, and $\gamma_3^3(p) = p\gamma$ also, for some integer γ. In this section we show that this, and related behaviour of more general orders, cannot happen. We first introduce some terminology.

Definition 1. For a fixed integer $M \geqslant 2$, a prime $p \equiv 1 \pmod M$ will be called α-*exceptional for* M if for the integer $\alpha \geqslant 1$ the second alternative in the appropriate case in (1.5) or (1.6) holds, or equivalently, if $T_\alpha^M(p) \equiv 0 \pmod p$; see (1.10).

Thus, all the primes listed in Table 1 are 1-exceptional for the appropriate M. The following result shows that the levels of exceptionality are strongly related with each other.

Theorem 3. *Let $M \geqslant 2$ be fixed. If, for an integer $\alpha \geqslant 2$, a prime $p \equiv 1 \pmod{M}$ is α-exceptional for M, then it is also $(\alpha-1)$-exceptional for M.*

We see that Examples 1 and 2 are consistent with this result which applies vacuously to these situations. On the other hand, this theorem shows that the hypothetical situation at the beginning of this section cannot occur since the 2-exceptionality of p would imply its 1-exceptionality. In other words, the only possible sequence of orders is (in the case of (1.5)) of the form

$$\gamma, \gamma, \ldots, \gamma, \gamma p, \gamma p^2, \gamma p^3, \ldots \qquad \text{or} \qquad \gamma, \gamma, \gamma, \ldots,$$

with the appropriate adjustments in the situations of (1.6). As mentioned before, we have not found any prime that is 2-exceptional for some $M \geqslant 3$. It is now a routine computation to check that none of the entries in Table 1 (and in Table 3 in [4]) are 2-exceptional.

For $M = 2$, on the other hand, *every* odd prime is α-exceptional for all $\alpha \geqslant 1$, which is again consistent with Theorem 3. This follows immediately from Theorem 2 in [2] and is related to the fact that $\gamma_\alpha^2(p)$ can only be 1, 2 or 4.

For the proof of Theorem 3 we need the following easy lemma.

Lemma 1. *Let p be an odd prime and $\alpha \geqslant 2$ an integer. Then the congruence $X^p \equiv 1 \pmod{p^\alpha}$ implies $X \equiv 1 \pmod{p^{\alpha-1}}$.*

Proof. When $X = 1$, the lemma is trivially true; we therefore assume that $X \neq 1$. By the first congruence we have $X^p \equiv 1 \pmod{p}$, and in particular $X \not\equiv 0 \pmod{p}$. Fermat's little theorem then gives $X^{p-1} \equiv 1 \pmod{p}$, and upon subtracting we get $X^p - X^{p-1} = (X-1)X^{p-1} \equiv 0 \pmod{p}$, which implies $X \equiv 1 \pmod{p}$.

Now let $a \in \mathbb{N}$ be such that $X = 1 + mp^a$ with an integer $m \not\equiv 0 \pmod{p}$. Then a binomial expansion gives

$$X^p = 1 + pmp^a + \sum_{j=2}^{p-1} \binom{p}{j} m^j p^{ja} + m^p p^{pa}. \tag{2.1}$$

Since $p \mid \binom{p}{j}$ for $1 \leqslant j \leqslant p-1$ and then $1 + ja \geqslant a + 2$ for all $j \geqslant 2$ and $a \geqslant 1$, the middle sum in (2.1) is divisible by p^{a+2}. Similarly, since p is odd, we have $pa \geqslant 3a \geqslant a + 2$ for $a \geqslant 1$, so that $p^{a+2} \mid p^{pa}$. Hence (2.1) gives

$$X^p \equiv 1 + mp^{a+1} \pmod{p^{a+2}},$$

which, by our hypothesis, means that $a \geqslant \alpha - 1$. It follows that $X \equiv 1 \pmod{p^{\alpha-1}}$, as desired. ∎

We note that the condition in Lemma 1 that p be an odd prime is necessary. Indeed, we have $3^2 \equiv 1 \pmod{2^3}$, but $3 \not\equiv 1 \pmod{2^2}$.

Proof of Theorem 3. If p is α-exceptional, then the expression in (1.10) vanishes modulo p. To obtain a contradiction, we assume that p is *not* $(\alpha-1)$-exceptional, where $\alpha \geqslant 2$. Then by definition, the first alternatives in (1.5) and (1.6) hold, with α replaced by $\alpha - 1$. In particular, since p is odd, we have in all cases $\gamma_\alpha^M(p) \equiv 0 \pmod{p}$. By our first statement above, which concerned the term in (1.10), this means that

$$V_\alpha^M(p) \equiv 0 \pmod{p}.$$

But then, the definition (1.9) of $V_\alpha^M(p)$ implies

$$\left(\left(\frac{p^\alpha-1}{M}\right)_p!\right)^{\gamma_\alpha^M(p)} \equiv 1 \pmod{p^{\alpha+1}}. \tag{2.2}$$

By our assumption that p is not $(\alpha-1)$-exceptional, we have once again

$$\gamma_\alpha^M(p) = \delta p \gamma_{\alpha-1}^M(p), \qquad \delta = \tfrac{1}{2}, 1, \text{or } 2.$$

We now use this relation and apply Lemma 1 to (2.2), obtaining

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

However, this contradicts the fact that, by the definition of the order, the smallest exponent giving $1 \pmod{p^\alpha}$ is $\gamma_\alpha^M(p) = p\cdot(\delta\gamma_{\alpha-1}^M(p))$. The proof is now complete. ∎

3. Some fundamental congruences for $M = 3$ and 6

In this section we derive a number of congruences that will be required in the following sections. Before we can state and prove our results, we need some facts related to the representation of a prime $p \equiv 1 \pmod 6$ in the form $p = a^2 + 3b^2$. It is known that this representation is unique up to signs, but the signs of a and b are crucial here and require some explanation (see [1, pp. 103–106]):

Let g be a primitive root modulo p and χ_6 a character modulo p of order 6 with $\chi_6(g) = e^{2\pi i/6} = (1+i\sqrt{3})/2$. Then we fix the signs of a and b 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 pairs r, s and u, v of integers as follows. Let $Z = \operatorname{ind}_g 2$, the index of $2 \pmod p$ with respect to g. Then

$$r = 2a, \quad s = 2b; \quad u = 2a, \quad v = 2b \qquad (Z \equiv 0 \pmod 3), \tag{3.1}$$

$$r = -a-3b, \ s = a-b; \quad u = -a+3b, \ v = -a-b \qquad (Z \equiv 1 \pmod 3), \tag{3.2}$$

$$r = -a+3b, \ s = -a-b; \ u = -a-3b, \ v = a-b \qquad (Z \equiv 2 \pmod 3). \tag{3.3}$$

We mention in passing that the integers r, s and u, v also satisfy sums-of-squares identities, namely

$$4p = r^2 + 3s^2 \qquad \text{and} \qquad 4p = u^2 + 3v^2, \qquad r \equiv u \equiv 1 \pmod 3 \tag{3.4}$$

We are now ready to state our results. In [3, Theorem 8] a well-known congruence of Jacobi for binomial coefficients, namely

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p, \tag{3.5}$$

was extended as follows: For any integer $\alpha \geqslant 1$ and for any prime $p \equiv 1 \pmod 6$ and integer r as defined in (3.1)–(3.3) we have

$$\frac{\left(\frac{2(p^{\alpha+1}-1)}{3}\right)_p!}{\left(\left(\frac{p^{\alpha+1}-1}{3}\right)_p!\right)^2} \equiv -J_\alpha(p) \pmod{p^{\alpha+1}}, \tag{3.6}$$

where for ease of notation we set

$$J_\alpha(p) := r - \frac{p}{r} - \frac{p^2}{r^3} - \cdots - C_{\alpha-1}\frac{p^\alpha}{r^{2\alpha-1}}, \tag{3.7}$$

with $C_n := \frac{1}{n+1}\binom{2n}{n}$ the nth Catalan number, which is always an integer. In analogy to the theorem of Jacobi (and a similar one due to Gauss which will be mentioned later), the following congruence was proved by Hudson and Williams [10]; see also [1, p. 270].

Theorem 4 (Hudson and Williams). *Let $p \equiv 1 \pmod 6$ be a prime and u as defined in* (3.1)–(3.3). *Then*

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1}u \pmod p. \tag{3.8}$$

In analogy to (3.6) we have the following result, the proof of which we will only sketch since it is quite similar to the proofs in [3]. This result will be the basis of much of what follows.

Theorem 5. *Let $p \equiv 1 \pmod 6$ be a prime and u as defined in* (3.1)–(3.3). *Then for any integer $\alpha \geqslant 1$ we have*

$$\frac{\left(\frac{p^{\alpha+1}-1}{3}\right)_p!}{\left(\left(\frac{p^{\alpha+1}-1}{6}\right)_p!\right)^2} \equiv (-1)^{\frac{p-1}{6}+1}K_\alpha(p) \pmod{p^{\alpha+1}}, \tag{3.9}$$

where

$$K_\alpha(p) := u - \frac{p}{u} - \frac{p^2}{u^3} - \cdots - C_{\alpha-1}\frac{p^\alpha}{u^{2\alpha-1}} \tag{3.10}$$

and C_n denotes the nth Catalan number.

The proof of this result is based on deep connections between the Jacobi sum $J(\chi,\psi)$ over the finite field $\mathbb{F}_p$, with χ and ψ characters on $\mathbb{F}_p$, and the p-adic gamma function $\Gamma_p(z)$ which can be defined as the limit

$$\Gamma_p(z) = \lim_{n\to z} F(n) \qquad (z \in \mathbb{Z}_p), \tag{3.11}$$

where n runs through any sequence of positive integers p-adically approaching z, and $F(n)$ is defined by $F(0) := 1$ and

$$F(n) := (-1)^n \prod_{\substack{0<j<n \\ p\nmid j}} j \qquad (n \geqslant 1). \tag{3.12}$$

For further details on $J(\chi,\psi)$ and $\Gamma_p(z)$ we refer the reader to a brief exposition in [3] which in turn is based on more detailed explanations in [1].

Proof of Theorem 5 (Sketch). We follow the outline of the related proofs of Theorems 7 and 8 in [3]. With the character χ_6 as defined before (3.1), we use the appropriate entries in Table 3.1.2 in [1, p. 107]:

$$J(\chi_6,\chi_6) = (-1)^{\frac{p-1}{6}}\frac{1}{2}(u+iv\sqrt{3}), \tag{3.13}$$

$$J(\chi_6^5,\chi_6^5) = (-1)^{\frac{p-1}{6}}\frac{1}{2}(u-iv\sqrt{3}), \tag{3.14}$$

where u and v are as in (3.1)–(3.3). Recall that $4p = u^2+3v^2$.

If $\mathfrak{p}$ is a nonzero prime ideal in the ring $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ of integers of $\mathbb{Q}(\sqrt{-3})$ dividing the prime p, then by Theorem 2.1.14 in [1, p. 66] we have $J(\chi_6,\chi_6) \equiv 0 \pmod{\mathfrak{p}}$. We combine this congruence with (3.13) and raise both sides to the power α, obtaining

$$(u+iv\sqrt{3})^\alpha \equiv 0 \pmod{\mathfrak{p}^\alpha}.$$

Since this holds for any nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ dividing p, we may conclude that this congruence also holds modulo p^α. Indeed, we know that p either remains prime, or splits, or ramifies in $\mathbb{Q}(\sqrt{-3})$. Therefore we have

$$(u+iv\sqrt{3})^\alpha \in p^\alpha\mathbb{Z}[\tfrac{1+i\sqrt{3}}{2}], \quad \text{resp.} \quad (u+iv\sqrt{3})^{2\alpha} \in p^\alpha\mathbb{Z}[\tfrac{1+i\sqrt{3}}{2}],$$

in the first case and the other two cases, respectively. This means that in any case, after replacing α by $\alpha+1$,

$$(u+iv\sqrt{3})^{\alpha+1} \equiv 0 \pmod{p^{\alpha+1}}. \tag{3.15}$$

Next, using identity (9.3.7) in [1, p. 278], together with (3.11) and (3.12), we obtain in analogy to the proof of Theorem 7 in [3],

$$J(\chi_6^5,\chi_6^5) = \frac{\Gamma_p(1-\frac{1}{3})}{\Gamma_p(1-\frac{1}{6})^2} \equiv -\frac{\left(\frac{p^{\alpha+1}-1}{3}\right)_p!}{\left(\left(\frac{p^{\alpha+1}-1}{6}\right)_p!\right)^2} \pmod{p^{\alpha+1}}. \tag{3.16}$$

The right-hand side of this is minus the left-hand side of (3.9). The remainder of the proof is now almost identical with the corresponding parts of the proofs of Theorems 7 and 8 in [3]: Expand the left-hand side of (3.15), collect real and imaginary parts, and use (3.14). Using appropriate combinatorial identities, we finally obtain the right-hand side of (3.9). ■

We will now use Theorem 5 and elements in its proof to derive the following fundamental result which will also be very useful later on.

Theorem 6. *Let $p \equiv 1 \pmod 6$ be a prime and r, u as defined in* (3.1)–(3.3). *Then for all $\alpha \geqslant 1$ we have*

$$\left(r - \frac{p}{r} - \cdots - \frac{C_{\alpha-1}p^\alpha}{r^{2\alpha-1}}\right)^3 \equiv \left(u - \frac{p}{u} - \cdots - \frac{C_{\alpha-1}p^\alpha}{u^{2\alpha-1}}\right)^3 \pmod{p^{\alpha+1}}. \quad (3.17)$$

We obtain this congruence as a consequence of the following result.

Lemma 2. *Let g be a primitive root, and let χ_3 be a character modulo p of order 3 with $\chi_3(g) = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$. Furthermore, let χ_6 be the character of order 6 defined before* (3.1). *Then*

$$\left(J(\chi_3^2, \chi_3^2)\right)^3 = \left((-1)^{\frac{p-1}{6}} J(\chi_6^5, \chi_6^5)\right)^3. \quad (3.18)$$

Proof of Theorem 6. A key congruence in the proof of Theorem 8 in [3, p. 114] shows that the left-hand side of (3.6) is congruent to $-J(\chi_3^2, \chi_3^2)$ modulo $p^{\alpha+1}$, so that

$$J(\chi_3^2, \chi_3^2) \equiv J_\alpha(p) \pmod{p^{\alpha+1}}. \quad (3.19)$$

Similarly, combining (3.9) and (3.16), we have

$$J(\chi_6^5, \chi_6^5) \equiv -(-1)^{\frac{p-1}{6}} K_\alpha(p) \pmod{p^{\alpha+1}}. \quad (3.20)$$

Substituting (3.19) and (3.20) into (3.18), we immediately obtain (3.17). ■

Proof of Lemma 2. By Tables 3.1.1 and 3.1.2, respectively, in [1, p. 106–107], we have

$$J(\chi_3^2, \chi_3^2) = \frac{r - is\sqrt{3}}{2}, \qquad J(\chi_6^5, \chi_6^5) = (-1)^{\frac{p-1}{6}} \frac{u - iv\sqrt{3}}{2},$$

where r, s, u and v are as in (3.1)–(3.3). Hence (3.18) is equivalent to

$$(r - is\sqrt{3})^3 = (u - iv\sqrt{3})^3. \quad (3.21)$$

We distinguish between the following cases according to (3.1) and (3.2), (3.3):

(i) When $Z \equiv 0 \pmod 3$, then (3.21) is trivially true.

(ii) When $Z \equiv \pm 1 \pmod 3$, then (3.21) is equivalent to

$$(-a \mp 3b + i(\pm a - b)\sqrt{3})^3 = (-a \pm 3b + i(\mp a - b)\sqrt{3})^3,$$

where "upper" and "lower" signs correspond to each other. But this is easily verified, for instance by multiplying the expression in parentheses on the left by the 3rd root of unity $-\frac{1}{2} \pm \frac{i}{2}\sqrt{3}$, which gives the expression in parentheses on the right, thus completing the proof. ∎

The above proofs show that the expressions in parentheses in (3.17), rather than their 3rd powers, are congruent to each other (in fact, equal) if and only if the case (3.1) holds. The following elementary congruence can be seen as a supplement to Theorem 6 for the case $\alpha = 0$.

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

Proof. We consider the factorization $r^3 - u^3 = (r-u)(r^2+ru+u^2)$ and use the fact that by (3.1)-(3.3) we have either $r = u$, or else in both remaining cases,

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

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

Now that we have proved Theorem 6, we can use it to derive another very useful congruence.

Corollary 1. *For any prime* $p \equiv 1 \pmod 6$ *and integer* $\alpha \geqslant 1$ *we have*

$$\left(\left(\tfrac{p^\alpha-1}{3}\right)_p!\right)^{24} \equiv \left(\left(\tfrac{p^\alpha-1}{6}\right)_p!\right)^{12} \pmod{p^\alpha}. \tag{3.22}$$

Proof. For $\alpha = 1$ we cube (3.5) and (3.8) and combine the two by using Lemma 3. Similarly, for $\alpha \geqslant 2$ we cube both sides of (3.6) and (3.9), replace $\alpha+1$ by α, and combine the two by using (3.17). In all cases we then have, for $\alpha \geqslant 1$,

$$\left(\left(\tfrac{2(p^\alpha-1)}{3}\right)_p!\right)^3 \left(\left(\tfrac{p^\alpha-1}{6}\right)_p!\right)^6 \equiv \pm\left(\left(\tfrac{p^\alpha-1}{3}\right)_p!\right)^9 \pmod{p^\alpha}. \tag{3.23}$$

By a result of D. H. Lehmer [11, Theorem 4], the Gauss factorial $(\frac{2}{3}(p^\alpha-1))_p!$ has $\frac{2}{3}\varphi(p^\alpha)$ factors in its defining product. Similarly, $(\frac{1}{3}(p^\alpha-1))_p!$ has $\frac{1}{3}\varphi(p^\alpha)$ factors, which is an even number since $p \equiv 1 \pmod 6$. Hence by symmetry, the product of all integers strictly between $\frac{2}{3}(p^\alpha-1)$ and p^α, and not divisible by p, is congruent to $(\frac{1}{3}(p^\alpha-1))_p! \pmod{p^\alpha}$, and we obtain

$$\left(\tfrac{2(p^\alpha-1)}{3}\right)_p! \left(\tfrac{p^\alpha-1}{3}\right)_p! \equiv (p^\alpha-1)_p! \equiv -1 \pmod{p^\alpha}, \tag{3.24}$$

by the Gauss-Wilson theorem (1.2). Finally, we multiply both sides of (3.23) by $(\frac{p^\alpha-1}{3})_p!^3$ and apply (3.24) to the left-hand side. Then upon squaring both sides we obtain (3.22). ∎

In [4, p. 159] we observed, without proof, that the ratios of the orders $\gamma_1^6(p)/\gamma_1^3(p)$ (see (1.4)) can take on only the 18 different values in the set

$$R_{18} := \left\{ \frac{1}{24}, \frac{1}{12}, \frac{1}{8}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{3}{8}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, 1, \frac{4}{3}, \frac{3}{2}, 2, 3, 4, 6, 12 \right\}. \tag{3.25}$$

We will now use Corollary 1 to show that this observation is actually true in a more general setting.

Corollary 2. *Let $\alpha \geqslant 1$ be fixed. Then for any $p \equiv 1 \pmod 6$ the ratio of orders $\gamma_\alpha^6(p)/\gamma_\alpha^3(p)$ can only take on values from the set R_{18} in* (3.25).

Proof. We use the congruence (3.22), and for greater ease of notation we set

$$X = \left(\tfrac{p^\alpha - 1}{3}\right)_p !, \qquad Y = \left(\tfrac{p^\alpha - 1}{6}\right)_p !.$$

Clearly none of the numbers X, Y, 12 or 24 is divisible by p. We set $R := \operatorname{ord}_{p^\alpha} X$, $S := \operatorname{ord}_{p^\alpha} Y$, so that $X^R \equiv 1 \pmod{p^\alpha}$, $Y^S \equiv 1 \pmod{p^\alpha}$. Then, by (3.22),

$$Y^{12R} \equiv \left(X^R\right)^{24} \equiv 1 \pmod{p^\alpha}, \qquad X^{24S} \equiv \left(Y^S\right)^{12} \equiv 1 \pmod{p^\alpha},$$

which means that $S \mid 12R$ and $R \mid 24S$. But we are interested in

$$\frac{\gamma_\alpha^6(p)}{\gamma_\alpha^3(p)} = \frac{S}{R} = \frac{s}{r},$$

where $r := R/d, s := S/d$, with $d := \gcd(R, S)$. So we have the conditions $s \mid 12r$, $r \mid 24s$, $\gcd(r, s) = 1$. This, in turn, means that s can only be a divisor of 12 and r a divisor of 24. It is now easy to check that the elements of the set R_{18} are the only possible ratios. ∎

Computations show that all 18 values in R_{18} are actually realized by ratios $\gamma_1^6(p)/\gamma_1^3(p)$.

Our next result brings us back to the concept of an α-exceptional prime for M, as defined at the beginning of Section 3. Also recall the numbers $T_\alpha^M(p)$ as defined in (1.10).

Theorem 7. *Let $p \equiv 1 \pmod 6$ be a prime, $\alpha \geqslant 1$ an integer, and let*

$$\frac{\gamma_\alpha^6(p)}{\gamma_\alpha^3(p)} = \frac{A_\alpha(p)}{B_\alpha(p)} \in R_{18}.$$

Then

$$2A_\alpha(p)T_\alpha^3(p) \equiv B_\alpha(p)T_\alpha^6(p) \pmod p. \tag{3.26}$$

Before we prove this result, we note that for $\alpha = 1$ this reduces to the congruence

$$2\gamma_1^6(p)T_1^3(p) \equiv \gamma_1^3(p)T_1^6(p) \pmod p$$

since neither one of $\gamma_1^6(p), \gamma_1^3(p)$ is divisible by p. This congruence was in fact obtained in [4] by different means.

As an immediate consequence of Theorem 7 we get the following result; it comes from the fact that by (3.26), $T^3_\alpha(p)$ and $T^6_\alpha(p)$ are either both zero or both nonzero modulo p.

Corollary 3. *Let $p \equiv 1 \pmod 6$ be a prime and $\alpha \geqslant 1$. Then p is α-exceptional for $M = 3$ if and only if it is α-exceptional for $M = 6$.*

Proof of Theorem 7. We raise the congruence (1.11) to the power 24, obtaining

$$\left(\left(\tfrac{p^{\alpha+1}-1}{3}\right)_p!\right)^{24\gamma^3_\alpha(p)} \equiv 1 + 24T^3_\alpha(p)p^\alpha \pmod{p^{\alpha+1}}. \tag{3.27}$$

The companion identity of (1.11) for $M = 6$, obtained in analogy to the proof of Proposition 2.2 in [4], is

$$\left(\left(\tfrac{p^{\alpha+1}-1}{6}\right)_p!\right)^{\gamma^6_\alpha(p)} \equiv \pm\left(1 + T^6_\alpha(p)p^\alpha\right) \pmod{p^{\alpha+1}}, \tag{3.28}$$

and raising this to the 12th power we get

$$\left(\left(\tfrac{p^{\alpha+1}-1}{6}\right)_p!\right)^{12\gamma^6_\alpha(p)} \equiv 1 + 12T^6_\alpha(p)p^\alpha \pmod{p^{\alpha+1}}. \tag{3.29}$$

Now, using the definition of $A_\alpha(p), B_\alpha(p)$ in the statement of the theorem, we let m be the common value of $A_\alpha(p)\gamma^3_\alpha(p) = B_\alpha(p)\gamma^6_\alpha(p)$. If we raise both sides of (3.27) to the power $A_\alpha(p)$ and (3.29) to the power $B_\alpha(p)$, then the left-hand sides are the mth powers of the two sides of (3.22), respectively (with α replaced by $\alpha + 1$) and are thus congruent to each other modulo $p^{\alpha+1}$. Then the right-hand sides of (3.27), (3.17) give, after the usual binomial expansion,

$$1 + 24A_\alpha(p)T^3_\alpha(p)p^\alpha \equiv 1 + 12B_\alpha(p)T^6_\alpha(p)p^\alpha \pmod{p^{\alpha+1}}.$$

Finally, we subtract 1 from both sides and divide by p^α, which gives (3.26). ∎

4. Tests for exceptionality for $M = 3$, 4 and 6

It can be seen from the definitions of the various functions of p in the criterion (1.10) that determining exceptionality in this way is computationally expensive. This is the case even when $M = 3$, 4 or 6, where the sums $S^M(p)$ can be written, modulo p, in terms of Fermat quotients which are easy to compute.

It is the main purpose of this section to give much simpler tests for exceptionality at all levels for $M = 3$, 4 and 6. These tests then allow us to carry the search for exceptional primes substantially further.

We begin with the cases $M = 3$ and 6; they are somewhat different from the case $M = 4$ which will be treated later in this section. As we will see, most of the key results of the previous section will be used in the proof of our first theorem.

Theorem 8. *Let $p \equiv 1 \pmod 6$ be a prime and u as defined in (3.1)–(3.3). Then for a fixed $\alpha \geqslant 1$, p is α-exceptional for $M = 3$ and also for $M = 6$ if and only if*

$$\left(u - \frac{p}{u} - \frac{p^2}{u^3} - 2\frac{p^3}{u^5} - \cdots - C_{\alpha-1}\frac{p^\alpha}{u^{2\alpha-1}}\right)^{p-1} \equiv 1 \pmod{p^{\alpha+1}}, \tag{4.1}$$

where C_n is the nth Catalan number.

Proof. We assume that p is α-exceptional for $M = 3$ and (by Corollary 3) equivalently for $M = 6$. Then by the definitions of $\gamma_\alpha^3(p)$ and $\gamma_\alpha^6(p)$, together with Theorem 3, we have $p - 1 = q\gamma_\alpha^3(p) = Q\gamma_\alpha^6(p)$ for some $q, Q \in \mathbb{N}$. Then with (3.9), (1.11) and (3.28) we get, after using binomial expansions in numerator and denominator,

$$K_\alpha(p)^{p-1} \equiv \frac{\left(\left(\frac{p^{\alpha+1}-1}{3}\right)_p!\right)^{q\gamma_\alpha^3(p)}}{\left(\left(\frac{p^{\alpha+1}-1}{6}\right)_p!\right)^{2Q\gamma_\alpha^6(p)}} \equiv \frac{1 + qT_\alpha^3(p)p^\alpha}{1 + 2QT_\alpha^6(p)p^\alpha} \pmod{p^{\alpha+1}}, \tag{4.2}$$

where $K_\alpha(p)$ is defined by (3.10), i.e., the left-hand sides of (4.2) and (4.1) are identical. Now, by Theorem 2, exceptionality means $T_\alpha^3(p) \equiv T_\alpha^6(p) \equiv 0 \pmod p$, which implies that the right-most term in (4.2) is congruent to $1 \pmod{p^{\alpha+1}}$, so (4.1) holds.

Conversely, suppose that (4.1) holds. Then (4.1) with (3.9) (or the left congruence of (4.2)) gives

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

On the other hand, raising both sides of the congruence (3.22) to the (integer) power $(p-1)/6$, we obtain

$$\left(\left(\frac{p^{\alpha+1}-1}{3}\right)_p!\right)^{4(p-1)} \equiv \left(\left(\frac{p^{\alpha+1}-1}{6}\right)_p!\right)^{2(p-1)} \pmod{p^{\alpha+1}}.$$

Combining these last two congruences, we get

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

Since $3(p-1) \not\equiv 0 \pmod p$ then $\gamma_{\alpha+1}^3(p) \not\equiv 0 \pmod p$; thus p is α-exceptional for $M = 3$ and by Corollary 3 also for $M = 6$. ∎

For computational purposes, and in view of Theorem 3, the case $\alpha = 1$ is of particular significance; we therefore state it as a separate result.

Corollary 4. *Let $p \equiv 1 \pmod 6$ be a prime and u as defined in (3.1)–(3.3). Then p is 1-exceptional for $M = 3$ and also for $M = 6$ if and only if*

$$\left(u - \tfrac{p}{u}\right)^{p-1} \equiv 1 \pmod{p^2}. \tag{4.3}$$

Although in the proof of Theorem 8 the use of the integer u was essential, Theorem 6 shows that it can be replaced by r, where both are defined in (3.1)–(3.3). We now give an elementary proof of this fact in the case $\alpha = 1$, and we also show that in this case we can replace r or u by $2a$, where a is uniquely determined by $p = a^2 + 3b^2$, $a \equiv -1 \pmod 3$.

Lemma 4. *Let $p \equiv 1 \pmod 6$, a as above, and u, r as defined in (3.1)–(3.3). Then*

$$\left(r - \tfrac{p}{r}\right)^3 \equiv \left(u - \tfrac{p}{u}\right)^3 \equiv \left(2a - \tfrac{p}{2a}\right)^3 \pmod{p^2}. \tag{4.4}$$

Proof. To prove the first congruence, we note that it is equivalent to

$$r^3 - 3rp \equiv u^3 - 3up \pmod{p^2},$$

or, upon rearranging and factoring, to

$$(r-u)(r^2 + ru + u^2) \equiv 3p(r-u) \pmod{p^2}. \tag{4.5}$$

If $r = u$, the congruences are trivially true; so we consider the case $r \neq u$. In this case r and u are given by (3.2) or (3.3), namely $r = -a \pm 3b$, $u = -a \mp 3b$. Upon expanding we obtain in both cases $r^2 + ru + u^2 = 3(a^2 + 3b^2) = 3p$, so that (4.5) holds again.

In analogy to (4.5) the second congruence in (4.4) is equivalent to

$$(u-2a)(u^2 + 2au + 4a^2) \equiv 3p(u-2a) \pmod{p^2}. \tag{4.6}$$

Here we have either $u = 2a$, in which the congruences hold trivially, or u is defined by (3.2) or (3.3), namely $u = -a \pm 3b$. We then obtain $u^2 + 2au + 4a^2 = 3(a^2 + 3b^2) = 3p$, and (4.6) holds again, and the proof is complete. ∎

By raising all three terms in (4.4) to the (integer) power $\frac{p-1}{3}$, we see that Corollary 4 remains true if in (4.3) we replace u by r or by $2a$. The latter case will be particularly useful for computations, and by expanding the left-hand side we immediately obtain the following criterion.

Corollary 5. *Let $p \equiv 1 \pmod 6$ be a prime and write $p = a^2 + 3b^2$ with $a \equiv -1 \pmod 3$. Then p is 1-exceptional for $M = 3$ and also for $M = 6$ if and only if*

$$(2a)^{p-3}\left((2a)^2 + p\right) \equiv 1 \pmod{p^2}. \tag{4.7}$$

In our final section we will make a few remarks on how to use this congruence in the search for 1-exceptional primes. To complete the current section, we prove the $M = 4$ analogue of Theorem 8. The proof, however, will be quite different.

Theorem 9. *Let $p \equiv 1 \pmod 4$ be a prime and write $p = a^2 + b^2$, where a and b are integers with $a \equiv 1 \pmod 4$. Then for a fixed $\alpha \geqslant 1$, p is α-exceptional for $M = 4$ if and only if*

$$\left(2a - \frac{p}{2a} - \frac{p^2}{(2a)^3} - \cdots - C_{\alpha-1}\frac{p^\alpha}{(2a)^{2\alpha-1}}\right)^{p-1} \equiv 1 \pmod{p^{\alpha+1}}, \tag{4.8}$$

where C_n is the nth Catalan number.

Proof. We use Theorem 7 of [3], namely

$$\frac{\left(\frac{p^{\alpha+1}-1}{2}\right)_p!}{\left(\left(\frac{p^{\alpha+1}-1}{4}\right)_p!\right)^2} \equiv G_\alpha(p) \pmod{p^{\alpha+1}}. \tag{4.9}$$

where

$$G_\alpha(p) := 2a - \frac{p}{2a} - \frac{p^2}{(2a)^3} - \cdots - C_{\alpha-1}\frac{p^\alpha}{(2a)^{2\alpha-1}}.$$

In analogy to the argument following (3.23), we note that by a result of D. H. Lehmer [11, Theorem 4], the Gauss factorial $(\frac{1}{2}(p^{\alpha+1}-1))_p!$ has $\frac{1}{2}\varphi(p^{\alpha+1})$ factors in its defining product. This number of factors is obviously an integer; in fact it is easily seen to be an even integer as $p \equiv 1 \pmod 4$. Therefore the above Gauss factorial is by symmetry congruent modulo $p^{\alpha+1}$ to the product of all integers from $\frac{1}{2}(p^{\alpha+1}-1)+1$ to $p^{\alpha+1}-1$, excluding the multiples of p. Thus we have

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

again by the Gauss-Wilson theorem (1.2). We raise both sides of (4.9) to the 4th power and combine it with the square of this last congruence, obtaining

$$\left(\left(\frac{p^{\alpha+1}-1}{4}\right)_p!\right)^8 \equiv \frac{1}{G_\alpha(p)^4} \pmod{p^{\alpha+1}}.$$

Since p is relatively prime to 8 and to 4, we see that

$$\operatorname{ord}_{p^{\alpha+1}}\left(\left(\frac{p^{\alpha+1}-1}{4}\right)_p!\right) \not\equiv 0 \pmod p$$

(which, in light of Theorem 3, is equivalent to p being α-exceptional for $M = 4$) if and only if

$$\operatorname{ord}_{p^{\alpha+1}} G_\alpha(p) \not\equiv 0 \pmod p. \tag{4.10}$$

As before, we have by Euler's generalization of Fermat's little theorem,

$$G_\alpha(p)^{p^\alpha(p-1)} \equiv 1 \pmod{p^{\alpha+1}},$$

which immediately implies that (4.10) holds if and only if (4.8) holds, and we are done. ∎

For $\alpha = 1$ we get an obvious analogue of Corollary 4. A 1-exceptionality test for $M = 4$ would then be identical with the congruence (4.7), but for the prime p and the integer a satisfying $p = a^2 + b^2$, $a \equiv 1 \pmod 4$.

5. Further consequences

We begin by briefly returning to the general case of $M \geqslant 2$. In Theorem 2 we defined the integer $T_\alpha^M(p)$ and recalled that a prime $p \equiv 1 \pmod M$ is α-exceptional for M if and only if $T_\alpha^M(p) \equiv 0 \pmod p$. However, in the case where $T_\alpha^M(p) \not\equiv 0 \pmod p$ (for some $\alpha \geqslant 1$) we did not say anything about the actual values (modulo p) of the $T_\beta^M(p)$, $\beta \geqslant \alpha$. Far from being arbitrary nonzero, these values behave in a very regular fashion, namely

$$\{T_\beta^M(p)\}_{\beta\geqslant\alpha} = \begin{cases} \{T, T, T, \ldots\}, \text{or} \\ \{T, \frac{1}{2}T, T, \frac{1}{2}T, \ldots\}, \text{or} \\ \{T, 2T, T, 2T, \ldots\}, \end{cases} \tag{5.1}$$

where $T = T_\alpha^M(p)$. We skip the proof of this fact, which is a fairly straightforward application of congruences such as (1.9) and a general version of (1.11).

In some special cases for $M = 3$ we can actually say more. We begin by quoting the following result from the forthcoming paper [7]; see also [5, p. 824]. We will refer to the integer r as defined in (3.1)–(3.3).

(i) Primes $p \equiv 1 \pmod 6$ for which the order of $\frac{p-1}{3}!$ is 1 or 3 are exactly those that are generated by $p = 3x^2 + 3x + 1$ and $x \equiv 1 \pmod 3$; equivalently, they are exactly those for which $r = 1$.

(ii) Primes $p \equiv 1 \pmod 6$ for which $\operatorname{ord}_p(\frac{p-1}{3}!) = 9$ are exactly those that are generated by the same quadratic $p = 3x^2 + 3x + 1$, but with $x \equiv 0$ or $2 \pmod 3$; equivalently, they are exactly those for which $\operatorname{ord}_p r = 3$.

Now, in connection with property (5.1), these primes also satisfy the following:

Theorem 10. *If the prime $p \equiv 1 \pmod 6$ satisfies $\operatorname{ord}_p(\frac{p-1}{3}!) = 3^\nu$ for $\nu = 0, 1$ or 2, then $T_1^3(p) \equiv 3^{\nu-1} \pmod p$. In particular, no prime of the form $p = 3x^2+3x+1$, $x \in \mathbb{N}$, is 1-exceptional for $M = 3$ and $M = 6$.*

Proof. By (1.11) with $\alpha = 1$ we have

$$\left(\left(\frac{p^2-1}{3}\right)_p!\right)^{\gamma_1^3(p)} \equiv 1 + T_1^3(p)p \pmod{p^2}, \tag{5.2}$$

and combining (3.24) for $\alpha = 2$ with (3.6) and (3.7) for $\alpha = 1$, we get

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

We first assume that $\nu = 0$ or 1. Then by case (i) preceding the theorem we have $r = 1$, and thus (5.3) gives

$$\left(\left(\tfrac{p^2-1}{3}\right)_p!\right)^3 \equiv 1 + p \pmod{p^2}. \tag{5.4}$$

When $\nu = 0$, i.e., $\gamma_1^3(p) = 1$, we cube (5.2), and its right-hand side becomes $1+3T_1^3(p)p \pmod{p^2}$. Comparing this with (5.4), we immediately get $T_1^3(p) \equiv 1/3 \pmod{p}$, as desired. Similarly, when $\nu = 1$, i.e., $\gamma_1^3(p) = 3$, then (5.2) and (5.4) immediately give $T_1^3(p) \equiv 1 \pmod{p}$, again as desired.

Second, we assume that $\nu = 2$; then by case (ii) above $\operatorname{ord}_p r = 3$. Now an easy binomial expansion gives $(r - p/r)^3 \equiv r^3 - 3pr \pmod{p^2}$, so if we can show that

$$r^3 - 3pr \equiv 1 - 3p \pmod{p^2}, \tag{5.5}$$

then by cubing both sides of (5.3) we would have

$$\left(\left(\tfrac{p^2-1}{3}\right)_p!\right)^9 \equiv \frac{1}{1-3p} \equiv 1 + 3p \pmod{p^2}.$$

Comparing this with (5.2), where $\gamma_1^3(p) = 9$, we immediately get $T_1^3(p) \equiv 3 \pmod{p}$, as desired.

It remains to verify (5.5). From $r^3 \equiv 1 \pmod{p}$ we have $(r-1)(r^2+1+1) \equiv 0 \pmod{p}$. But $r \not\equiv 1 \pmod{p}$ since the order is 3, so we have $r^2 + r + 1 = mp$ for some $m \in \mathbb{N}$. First we note that m has to be odd since $r^2 + r + 1$ is. Next, since $r \equiv 1 \pmod{3}$ (see (3.4)) we have $3 \mid r^2 + r + 1$, so $m = 1$ is impossible. Finally, from $4p = r^2 + 3s^2$ (see (3.4) again) we have $r^2 < 4p$ and thus

$$r^2 + r + 1 < 4p + 2\sqrt{p} + 1 = \left(4 + \frac{2}{\sqrt{p}} + \frac{1}{p}\right)p,$$

so $m < 5$ for $p \geqslant 7$. This leaves $m = 3$ as the only possibility, i.e., we have $r^2 + r + 1 = 3p$. But this implies

$$r^3 - 3pr = r^3 - r(r^2 + r + 1) = -r^2 - r = 1 - 3p,$$

so (5.5) is actually an equality.

The final statement of the theorem follows from the remarks preceding it, and from Theorem 2 and Corollary 3. ■

We now turn to a class of primes, generated in a similar fashion to those in Theorem 10, that have the opposite property in that they are *all* 1-exceptional. In [4] we gave a rather involved proof of the following result which is now an easy consequence of Corollary 4.

Corollary 6. *Every prime p such that $p^2 = 3x^2 + 3x + 1$ for some integer x is 1-exceptional for $M = 3$ and $M = 6$.*

Proof. In [4, p. 169] we showed that the given primes satisfy

$$\left(r - \tfrac{p}{r}\right)^6 \equiv -1 \pmod{p^2}. \tag{5.6}$$

In particular, this congruence shows that -1 is a quadratic residue modulo p, and thus $p \equiv 1 \pmod 4$. This means that $\frac{1}{6}(p-1)$ is even, and from (5.6) we get

$$\left(r - \tfrac{p}{r}\right)^{p-1} \equiv (-1)^{\frac{p-1}{6}} = 1 \pmod{p^2}.$$

Corollary 4 now shows that p is 1-exceptional for $M = 3$ and $M = 6$. ■

Primes that satisfy $p^2 = 3x^2 + 3x + 1$ account for all of the entries in Table 1 for $M = 3$ and $M = 6$, with the sole exception of $p = 76\,543$. Following Theorem 3 we remarked that we checked all entries in Table 1 and found that they are not 2-exceptional. For $M = 3$ and $M = 6$, all entries except $p = 76\,543$ are of the type already considered in Corollary 6 above. For these primes we can actually *prove* that they are not 2-exceptional.

Theorem 11. *Suppose the prime p is such that $p^2 = 3x^2 + 3x + 1$ for some integer x. Then p is not 2-exceptional for $M = 3$ or $M = 6$.*

Before we can use Theorems 8 and 6 to prove this result, we need the following technical lemma.

Lemma 5. *Let p be a prime such that $p^2 = 3x^2 + 3x + 1$ for some integer x, and let r be defined by* (3.1)–(3.3)*. Then*

$$r^2(r^2 - 3p)^2 = (p+1)^2(2p-1). \tag{5.7}$$

Proof. The equation $p^2 = 3x^2 + 3x + 1$ can be rewritten in the form of the Pell equation $(2p)^2 - 3(2x+1)^2 = 1$, and from the theory of these equations (see, e.g., [14, Section 7.8]) we get

$$p = \frac{1}{2}A_{2k-1}, \tag{5.8}$$

where the sequence $\{A_j\}$ is defined by $A_0 = 1$, $A_1 = 2$, and

$$A_{n+1} = 4A_n - A_{n-1} \qquad (n \geqslant 1). \tag{5.9}$$

Properties of this well-known sequence can be found, e.g., in [15, A001075], and they include the identities

$$2A_{k-1}A_k = A_{2k-1} + 2, \qquad A_{k-1}A_{k+1} - A_k^2 = 3 \qquad (k \geqslant 1); \tag{5.10}$$

see also [4, p. 165] for further properties and a small table. Combining the second identity in (5.10) with (5.9), we obtain

$$A_k^2 - 4A_kA_{k-1} + A_{k-1}^2 + 3 = 0 \qquad (k \geqslant 1), \tag{5.11}$$

which will also be useful.

Now, in addition to p in (5.8), the integer r can also be expressed in terms of the sequence $\{A_j\}$; see [4, Lemma 9]: If $p = \frac{1}{2}A_{2k-1}$ is a prime, then

$$r = \begin{cases} (-1)^k A_k & \text{if} \quad 2k-1 \equiv 1 \pmod 3, \\ (-1)^{k-1} A_{k-1} & \text{if} \quad 2k-1 \equiv -1 \pmod 3. \end{cases} \tag{5.12}$$

We are now ready to prove (5.7). We first consider the case $2k-1 \equiv 1 \pmod 3$. Then $r^2 = A_k^2$, and with (5.8) the identity (5.7) is equivalent to

$$A_k^2 \left(A_k^2 - \tfrac{3}{2}A_{2k-1}\right)^2 = \left(\tfrac{1}{2}A_{2k-1} + 1\right)^2 (A_{2k-1} - 1)\,.$$

Using the first identity in (5.10) to replace all occurrences of A_{2k-1}, we obtain after dividing both sides by A_k^2,

$$\left(A_k^2 - 3A_kA_{k-1} + 3\right)^2 = A_{k-1}^2 \left(2A_kA_{k-1} - 3\right). \tag{5.13}$$

Applying (5.11), the left-hand side of (5.13) becomes

$$\left(A_{k-1}A_k - A_{k-1}^2\right)^2 = A_{k-1}^2 \left(A_k^2 - 2A_kA_{k-1} + A_{k-1}^2\right),$$

and upon using (5.11) a second time, we see that this gives the right-hand side of (5.13). This completes the proof of (5.7) when $2k-1 \equiv 1 \pmod 3$.

In the second case, (5.12) gives $r^2 = A_{k-1}^2$, and the proof will be very similar, with only a small shift in the subscripts. ∎

Proof of Theorem 11. We first expand the left-hand term of the following congruence, reducing modulo p^3; then we use (5.7) and expand and reduce again:

$$\begin{aligned} \left(r - \frac{p}{r} - \frac{p^2}{r^3}\right)^6 &\equiv r^6 - 6r^4p + 9r^2p^2 = r^2\left(r^2 - 3p\right)^2 \pmod{p^3} \\ &= (p+1)^2(2p-1) \equiv 3p^2 - 1 \pmod{p^3}. \end{aligned}$$

Now we raise the left- and right-most sides to the power $\frac{1}{6}(p-1)$, noting that this is an even integer, as we saw in the proof of Corollary 6. Then expanding and reducing again, we get

$$\begin{aligned} \left(r - \frac{p}{r} - \frac{p^2}{r^3}\right)^{p-1} &\equiv \left(1 - 3p^2\right)^{\frac{p-1}{6}} \equiv 1 - \frac{p-1}{6}3p^2 \pmod{p^3} \\ &\equiv 1 + \frac{1}{2}p^2 \not\equiv 1 \pmod{p^3}. \end{aligned} \tag{5.14}$$

This means that, by Theorem 6 and Theorem 8, p is not 2-exceptional for $M = 3$ and $M = 6$. ∎

We finish this section with a few further remarks concerning primes that satisfy $p^2 = 3x^2 + 3x + 1$ for an integer x. First, by reducing (5.14) modulo p^2, we immediately get another proof of Corollary 6.

Next we note that as part of the very different proof in [4] of this last corollary, we showed that $\gamma_1^3(p) = \gamma_2^3(p) = 36$ when $p \neq 13$, and the common value is 12 when $p = 13$. Using this, together with much of the work in the previous two proofs, one can also show that $T_2^3(p) \equiv 6 \pmod{p}$ when $p \neq 13$, and $T_2^3(13) \equiv 4 \pmod{13}$.

Our final remark concerns the identity (5.8) which provides an easy way of obtaining primes satisfying $p^2 = 3x^2 + 3x + 1$. In [4, Lemma 7] we showed that a necessary condition for the primality of p is the primality of $2k-1$. It turns out that p is indeed prime for all odd primes $2k - 1 \leqslant 19$ (tabulated in [4, p. 166]), the first four of which appear in Table 1 of the present paper. But the next values $2k - 1$ for which p is prime are only 79, 151, 199, 233, 251, 317, 816 and 971; we also have probable primes for $2k - 1 = 3049$, 7451 and 7487. There are no more with $2k - 1 < 10\,000$, and the largest of these probable primes has 4282 decimal digits. It is reasonable to conjecture that there are infinitely many such primes.

6. Some final remarks

1. The quotient (1.3) is not always an integer unless $p \equiv 1 \pmod{M}$, but it is worth mentioning that by considering the floor function $\lfloor \frac{p^\alpha - 1}{M} \rfloor$, one can also define an appropriate analogue of the Gauss factorial in (1.3) for p in other residue classes modulo M. Such modified Gauss factorials and their orders were in fact studied in [4], Section 3. However, in the present paper we have, for the sake of simplicity and brevity, restricted our attention to primes $p \equiv 1 \pmod{M}$.

2. We conclude this paper with some notes on computations in the cases $M = 3, 6$ and $M = 4$. In both cases the congruence (4.7) is most convenient to use; when $M = 4$, however, we have $p = a^2 + b^2$ and $a \equiv 1 \pmod 4$, as opposed to the hypothesis of Corollary 5.

In practice we let a and b run through their respective residue classes of relevance, and then test (4.7) with p *defined* as $a^2 + 3b^2$ (respectively $a^2 + b^2$), whether or not p is prime. Only when a solution of (4.7) was found, we tested p for primality.

In this way we were able to check for 1-exceptionality in the case $M = 3$ (and thus also $M = 6$) for $p < 10^{12}$, and in the the case $M = 4$ for $p < 10^{11}$. The relevant entries in Table 1 are complete up to these limits.

The computations were all done with the computer algebra system Maple. Using our new exceptionality tests (as opposed to Theorem 2), we were able to reach the former search limits of $4 \cdot 10^8$ in under three minutes in each of the two cases. The new search limits in the two cases were reached in about 2 days of CPU time each, on a standard desktop computer. Obviously, one could reach higher search limits with a specially designed program, and also use opportunities for parallelization (as we did with Maple). However, the computational aspects were not the main focus of this paper.

Acknowledgments. We thank the anonymous referee for a very careful reading of this paper, and for helpful suggestions that led to its improvement.

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), no. 2, 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 Gauss–Wilson theorem for quarter-intervals*, Acta Math. Hungar. **142** (2014), no. 1, 199–230.

[7] J.B. Cosgrave and K. Dilcher, *A role for generalized Fermat numbers*, Math. Comp. (to appear).

[8] L.E. Dickson, *History of the Theory of Numbers. Volume I: Divisibility and Primality*, Chelsea, New York, 1966.

[9] Y. Gallot, Private communication, June, 2009.

[10] R.H. Hudson and K.S. Williams, *Binomial coefficients and Jacobi sums*, Trans. Amer. Math. Soc. **281** (1984), no. 2, 431–505.

[11] D.H. Lehmer, *The distribution of totatives*, Canad. J. Math. **7** (1955), 347–357.

[12] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. Oxford Ser. **3**9 (1938), 350–360.

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

[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/.

Addresses: John B. Cosgrave: 79 Rowanbyrn, Blackrock, County Dublin, Ireland;
Karl Dilcher: Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada.

E-mail: jbcosgrave@gmail.com, dilcher@mathstat.dal.ca

Received: 28 October 2014; **revised:** 7 May 2015