An Introduction to Gauss Factorials

John B. Cosgrave and Karl Dilcher

Abstract. Starting with Wilson's theorem and its generalization by Gauss, we define a Gauss factorial $N_n!$ to be the product of all positive integers up to N that are relatively prime to n. We present results on the Gauss factorials $(\frac{n-1}{M})_n!$, and more generally on partial products obtained when the product $(n-1)_n!$ is divided into M equal parts, for integers $M \geq 2$. Finally, extensions of the Gauss binomial coefficient theorem are presented in terms of Gauss factorials.

1. INTRODUCTION. One of the most remarkable results in elementary number theory is Wilson's theorem and its converse by Lagrange, stating that p is a prime if and only if

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

A proof of this result can be found in most introductory books on number theory, and it depends on the fact that if p is prime then any integer a with $1 < a < p-1$ has its inverse $a^{-1} \not\equiv a \pmod{p}$.

For any odd prime p, if we write out the factorial $(p-1)!$ and exploit symmetry modulo p, we obtain

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

and therefore, by (1.1),

$$\left(\tfrac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}. \tag{1.3}$$

This was apparently first observed by Lagrange (see [**13**, p. 275]), and this congruence can be used, along with a result of Mordell [**24**] that involves the class numbers of imaginary quadratic fields, to completely characterize the multiplicative order of $\left(\frac{p-1}{2}\right)!$ modulo p. We will leave this aside, and instead consider now the two halves of the product on the left-hand side of (1.2). We denote these two partial products by $\Pi_1^{(2)}$ and $\Pi_2^{(2)}$, respectively, where the upper index indicates the fact that we divide the entire product into two equal parts. Using Wilson's theorem (1.1) and symmetry modulo p, we obtain $\Pi_1^{(2)}\Pi_2^{(2)} \equiv -1 \pmod{p}$ and

$$\Pi_2^{(2)} \equiv (-1)^{\frac{p-1}{2}} \Pi_1^{(2)} \pmod{p}. \tag{1.4}$$

This is, of course, equivalent to (1.3), but writing it in this way gives rise to the following question:

What can we say about the three partial products $\Pi_1^{(3)}, \Pi_2^{(3)}, \Pi_3^{(3)}$ obtained by dividing the entire product $(p-1)!$, that is, the left-hand side of (1.1), into *three* equal parts? For this we require p to be of the form $p \equiv 1 \pmod{3}$ or, in fact (since p is prime), $p \equiv 1 \pmod{6}$; we then have

$$\Pi_1^{(3)} = 1 \cdot 2 \cdots \tfrac{p-1}{3}, \quad \Pi_2^{(3)} = \tfrac{p+2}{3} \cdots \tfrac{2p-2}{3}, \quad \Pi_3^{(3)} = \tfrac{2p+1}{3} \cdots (p-1).$$

http://dx.doi.org/10.4169/amer.math.monthly.118.09.812

In analogy to (1.4) we see an obvious symmetry relation between $\Pi_1^{(3)}$ and $\Pi_3^{(3)}$, namely

$$\Pi_3^{(3)} \equiv \Pi_1^{(3)} \pmod{p}, \tag{1.5}$$

but without a power of -1 since $\frac{p-1}{3}$ is always even. However, there is no obvious relation between $\Pi_1^{(3)}$ and the "middle third" $\Pi_2^{(3)}$.

Going one step further, for $p \equiv 1 \pmod 4$ we now divide the entire product $(p-1)!$ into *four* partial products

$$\Pi_j^{(4)} = \left((j-1)\tfrac{p-1}{4}+1\right)\left((j-1)\tfrac{p-1}{4}+2\right)\cdots\left(j\tfrac{p-1}{4}\right), \quad (j=1,2,3,4). \tag{1.6}$$

This time we have two obvious symmetry relations, namely

$$\Pi_4^{(4)} \equiv (-1)^{\frac{p-1}{4}}\Pi_1^{(4)} \pmod{p}, \quad \Pi_3^{(4)} \equiv (-1)^{\frac{p-1}{4}}\Pi_2^{(4)} \pmod{p}, \tag{1.7}$$

while there is no obvious relation between $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$.

Table 1 illustrates the congruences (1.5) and (1.7). We also see that, indeed, there are no obvious relationships between $\Pi_1^{(M)}$ and $\Pi_2^{(M)}$ for $M=3$ and 4 and $p<100$, with the exceptions of $p=7$ and $p=61$, where $\Pi_1^{(3)} \equiv -\Pi_2^{(3)} \pmod{p}$. These could, of course, be coincidences, but it turns out that this congruence holds also for $p=331$, $p=547$, $p=1951$, and for further relatively rare primes, as explained later. Here it is interesting to mention $p=3571$, the first case with $\Pi_1^{(3)} \equiv -\Pi_2^{(3)} \equiv 1 \pmod{p}$. In contrast, there are no primes p for which $\Pi_1^{(3)} \equiv \Pi_2^{(3)} \pmod{p}$, $p \equiv 1 \pmod 6$, or $\Pi_1^{(4)} \equiv \pm\Pi_2^{(4)} \pmod{p}$, $p \equiv 1 \pmod 4$. All this is readily explained by appealing to two deep theorems of Jacobi and of Gauss; we will return to this later.

Table 1. The partial products modulo p, for $(p-1)!$ split into $M=3$ and $M=4$ equal parts.

p	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	p	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
7	**2**	**−2**	**2**	5	1	2	−2	−1
13	−2	3	−2	13	6	3	−3	−6
19	−2	−5	−2	17	7	−3	−3	7
31	2	−8	2	29	−6	−2	2	6
37	7	3	7	37	−16	5	−5	16
43	−3	19	−3	41	13	7	7	13
61	**−14**	**14**	**−14**	53	26	7	−7	−26
67	−20	−33	−20	61	19	7	−7	−19
73	33	−12	33	73	18	−35	−35	18
79	−37	3	−37	89	22	42	42	22
97	21	−11	21	97	20	−28	−28	20

This naturally leads to the question of dividing the product $(p-1)!$ into 5, 6, or in general $M \geq 2$ partial products of equal length, for primes $p \equiv 1 \pmod{M}$. In analogy to (1.6) we define, for such M and p, the products

$$\Pi_j^{(M)} = \prod_{i=1}^{\frac{p-1}{M}} \left((j-1)\tfrac{p-1}{M}+i\right), \quad (j=1,2,\ldots,M). \tag{1.8}$$

Once again it is clear that

$$\Pi_{M-j}^{(M)} \equiv \pm\Pi_{j}^{(M)} \pmod p, \quad j = 1, 2, \ldots, \lfloor \tfrac{M-1}{2} \rfloor,$$

with the "central product" $\Pi_{(M+1)/2}^{(M)}$ playing a somewhat special role when M is odd. Extensive computations suggest that while (for fixed M) there are instances where two of the partial products, with $1 \le j \le \lfloor \frac{M+1}{2} \rfloor$, are congruent, there are no cases where all are simultaneously congruent.

2. COMPOSITE MODULI. This might well have been the end of the story were it not for the possibility of considering *composite* moduli. Since our point of departure has been Wilson's theorem (1.1), let us first recall why Lagrange's converse is true. If n is composite, we can write it as $n = n_1 n_2$, with $1 < n_1 < n$. But then $n_1 \mid (n-1)!$, and therefore $(n-1)! \not\equiv \pm 1 \pmod n$. However, if we suitably modify the factorial on the left-hand side of (1.1), we obtain a composite analogue of Wilson's theorem. It was Gauss who first proved the following theorem.

Theorem 1 (Gauss). *For any integer $n \ge 2$ we have*

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

where p is an odd prime and α is a positive integer.

The number of integers j in the product in (2.1), that is, those positive integers up to n that are relatively prime to n, is given by Euler's totient function $\phi(n)$, which has the explicit evaluation $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$, with the product taken over all prime divisors p of n. We recall that the integers n in (2.1) for which the product is -1 (mod n) are exactly those that have a primitive root; this fact is important for the proof of the result.

In spite of the fact that Theorem 1 was stated in the famous *Disquisitiones Arithmeticae* [**17**, §78] and in the equally influential books [**14**, §38] and [**20**, p. 102], surprisingly little can be found on this topic in the literature. The few published references to this result include [**21**] and [**27**], where Theorem 1 was further extended, and [**22**] and [**1**], where (2.1) was used to extend the classical *Wilson quotient* to composite moduli. The theorem was rediscovered at least once; see [**26**].

In order to state this theorem and numerous other results more concisely, we introduce the following notation: for positive integers N and n let $N_n!$ denote the product of all integers up to N that are relatively prime to n, i.e.,

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

This notation is a slight variation of the one used in [**18**], a useful reference on factorial and binomial congruences. To be able to refer more easily to $N_n!$, we shall call it a *Gauss factorial*, a terminology suggested by Theorem 1, which we call from here on the *Gauss-Wilson theorem.*

We now turn to the composite analogue of Lagrange's observation in (1.2) and (1.3) and begin with a general discussion of the Gauss factorial $\left(\frac{n-1}{2}\right)_n!$ for odd integers

$n \geq 3$. Since $(n-1)_n!$ is a product of $\phi(n)$ residues, and $\phi(n)$ is even for odd $n \geq 3$, then by the same symmetry argument as in (1.2) we obtain

$$\left(\tfrac{n-1}{2}\right)_n!^2 \equiv (-1)^{\frac{1}{2}\phi(n)+\varepsilon} \pmod{n}, \tag{2.3}$$

where, by (2.1), $\varepsilon = 1$ when $n = p^\alpha$, and $\varepsilon = 0$ otherwise. Now $\phi(p^\alpha) = (p-1)p^{\alpha-1}$, and therefore

$$\tfrac{1}{2}\phi(p^\alpha) + 1 \equiv \tfrac{p-1}{2} + 1 = \tfrac{p+1}{2} \pmod{2}.$$

On the other hand, $\phi(n)$ is divisible by 4 if n has at least two distinct odd prime factors. Hence by (2.3) we get

$$\left(\tfrac{n-1}{2}\right)_n!^2 \equiv \begin{cases} -1 \pmod{n} & \text{if} \quad n = p^\alpha,\ p \equiv 1 \pmod{4}, \\ 1 \pmod{n} & \text{otherwise.} \end{cases} \tag{2.4}$$

This is analogous to (1.3) for prime powers. In connection with this congruence we remark that the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined in [**7**].

As we did following (1.3), we will now turn to dividing the product $(n-1)_n!$ into partial products. In complete analogy to (1.8) we define our partial products $\Pi_j^{(M)}$, for integers $M \geq 2$ and $n \equiv 1 \pmod{M}$, as

$$\Pi_j^{(M)} := \prod_{i \in I_j^{(M)}} i, \quad (j = 1, 2, \ldots, M), \tag{2.5}$$

where, for $j = 1, 2, \ldots, M$,

$$I_j^{(M)} := \left\{ i \mid (j-1)\tfrac{n-1}{M} + 1 \leq i \leq j\tfrac{n-1}{M}, \gcd(i, n) = 1 \right\}. \tag{2.6}$$

The dependence on n, always considered a fixed modulus, is implied in this notation. When $n = p$ is prime, the definition (2.5) reduces to (1.8); the use of identical notation is therefore justified.

Table 1 could now be extended to include composite moduli. To save space, only the last ten cases with $n < 100$ for each of $M = 3$ and $M = 4$ are shown in Table 2. This immediately shows that, in contrast to the prime modulus case, the partial products can indeed all be congruent to each other modulo n. In particular, we see that this happens for $n = 91$ when $M = 3$, and for $n = 65$ and 85 when $M = 4$.

Table 2. Partial products modulo n, for 10 values of $n < 100$, $M = 3, 4$.

n	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	n	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
70	29	1	29	61	19	7	−7	−19
73	33	−12	33	65	**8**	**8**	**8**	**8**
76	−29	−15	−29	69	31	−26	−26	31
79	−37	3	−37	73	18	−35	−35	18
82	−33	−25	−33	77	16	31	31	16
85	−28	9	−28	81	2	40	−40	2
88	5	−7	5	85	**13**	**13**	**13**	**13**
91	**29**	**29**	**29**	89	22	42	42	22
94	−23	43	−23	93	34	−10	−10	34
97	21	−11	21	97	20	−28	−28	20

3. A QUESTION CONSIDERED BY D. H. LEHMER. Before explaining this last observation in Section 4, let us pause briefly to consider the sets $I_j^{(M)}$ defined in (2.6), and in particular their cardinalities

$$\phi_{M,j}(n) := \#I_j^{(M)}. \tag{3.1}$$

First, when $n = p$ is a prime, then clearly for a given M all $I_j^{(M)}$ have the same number of elements, namely $\phi_{M,j}(p) = \frac{p-1}{M}$. Next, when $M = 1$, then $\phi_{1,1}(n) = \phi(n)$. When $M = 2$, then by symmetry of the sets $I_1^{(2)}$ and $I_2^{(2)}$ we have $\phi_{2,1}(n) = \phi_{2,2}(n) = \frac{1}{2}\phi(n)$. However, already in the case $M = 3$ the situation is not as straightforward, as the example $n = 4$ shows: in this case we have $\phi_{3,1}(n) = \phi_{3,3}(n) = 1$, but $\phi_{3,2}(n) = 0$.

According to D. H. Lehmer [**23**] it was J. J. Sylvester who coined the term *totatives* for those positive integers up to a given n that are relatively prime to n. We are therefore dealing with the distribution of totatives in subintervals of the interval $[1, n]$. Lehmer [**23**] was the first to study this distribution, and to give a sufficient condition for the equal distribution of totatives. This area of study has attracted the attention of later mathematicians; for instance, a conjecture of Erdős [**16**] was proven by Hall and Shiu [**19**].

Table 3. The first ten moduli n for which all $\phi_{M,j}(n)$ are equal, for each of $M = 3, 4, 5$.

n	factored	$\phi_{3,j}$	n	factored	$\phi_{4,j}$	n	factored	$\phi_{5,j}$
28	$2^2 \cdot 7$	4	25	5^2	5	66	$2 \cdot 3 \cdot 11$	4
49	7^2	14	45	$3^2 \cdot 5$	6	121	11^2	22
52	$2^2 \cdot 13$	8	65	$5 \cdot 13$	12	176	$2^4 \cdot 11$	16
70	$2 \cdot 5 \cdot 7$	8	85	$5 \cdot 17$	16	186	$2 \cdot 3 \cdot 31$	12
76	$2^2 \cdot 19$	12	105	$3 \cdot 5 \cdot 7$	12	231	$3 \cdot 7 \cdot 11$	24
91	$7 \cdot 13$	24	117	$3^2 \cdot 13$	18	246	$2 \cdot 3 \cdot 41$	16
112	$2^4 \cdot 7$	16	125	5^3	25	286	$2 \cdot 11 \cdot 13$	24
124	$2^2 \cdot 31$	20	145	$5 \cdot 29$	28	341	$11 \cdot 31$	60
130	$2 \cdot 5 \cdot 13$	16	153	$3^2 \cdot 17$	24	366	$2 \cdot 3 \cdot 61$	24
133	$7 \cdot 19$	36	165	$3 \cdot 5 \cdot 11$	20	396	$2^2 \cdot 3^2 \cdot 11$	24

Table 3 seems to indicate that whenever $n \equiv 1 \pmod{M}$ has a prime factor p satisfying $p \equiv 1 \pmod{M}$, then the corresponding totatives are equally distributed, that is, all $\phi_{M,j}(n)$ are equal. This is in fact true, as was shown by D. H. Lehmer [**23**, Theorem 4]:

Lemma 1 (Lehmer). *Let $M \geq 2$ and $n \equiv 1 \pmod{M}$. If n has at least one prime factor p with $p \equiv 1 \pmod{M}$, then the totatives in the interval $[1, n]$ are equally distributed, that is, we have*

$$\phi_{M,j}(n) = \frac{1}{M}\phi(n), \quad (j = 1, 2, \ldots, M). \tag{3.2}$$

Lehmer actually showed something slightly different, namely that under the given conditions the intervals

$$(j-1)\frac{n}{M} < i < j\frac{n}{M}, \quad j = 1, 2, \ldots, M, \tag{3.3}$$

have equal numbers of integers i relatively prime to n, and the endpoints cannot themselves be totatives. However, we can easily see that this implies Lemma 1. For further details, see [**7**, Lemma 2]. This lemma is an important ingredient in a proof in the next section.

While Lehmer's theorem gives a sufficient condition, the following example shows that it is not necessary: Let $M = 8$ and $n = 105 = 3 \cdot 5 \cdot 7$. Although none of the prime factors of n are of the form $p \equiv 1 \pmod{8}$, a computation shows that each of the eight sets $I_j^{(8)}$ contains $\frac{1}{8}\phi(105) = 6$ elements.

4. THE CASE WHERE THE PARTIAL PRODUCTS ARE ALL CONGRUENT.

In order to further explore the case where all partial products $\Pi_j^{(M)}$, for a fixed M, are congruent to each other modulo n, we computed many pairs of M and n for which this is the case. Table 4 shows the first ten such moduli n for each of $M = 3$, 4, and 5, along with the factorizations of n and the common values

$$\left(\tfrac{n-1}{M}\right)_n! \equiv \Pi_j^{(M)} \pmod{n}, \quad j = 1, 2, \dots, M. \tag{4.1}$$

By definition the left-hand side of (4.1) is obviously identical with the right-hand side for $j = 1$.

Table 4. The first ten moduli n for which all $\Pi_j^{(M)}$ are congruent, for each of $M = 3, 4, 5$.

n	factored	$\Pi_j^{(3)}$	n	factored	$\Pi_j^{(4)}$	n	factored	$\prod_j^{(5)}$
91	$7 \cdot 13$	29	65	$5 \cdot 13$	8	341	$11 \cdot 31$	-85
133	$7 \cdot 19$	58	85	$5 \cdot 17$	13	451	$11 \cdot 41$	-105
217	$7 \cdot 31$	67	145	$5 \cdot 29$	1	671	$11 \cdot 61$	-304
244	$2^2 \cdot 61$	1	185	$5 \cdot 37$	-68	781	$11 \cdot 71$	-117
247	$13 \cdot 19$	-88	205	$5 \cdot 41$	1	1111	$11 \cdot 101$	36
259	$7 \cdot 37$	100	221	$13 \cdot 17$	-1	1271	$31 \cdot 41$	264
301	$7 \cdot 43$	36	265	$5 \cdot 53$	23	1441	$11 \cdot 131$	89
364	$2^2 \cdot 7 \cdot 13$	113	305	$5 \cdot 61$	-121	1661	$11 \cdot 151$	-545
403	$13 \cdot 31$	118	325	$5^2 \cdot 13$	-57	1891	$31 \cdot 61$	497
427	$7 \cdot 61$	135	365	$5 \cdot 73$	27	1991	$11 \cdot 181$	125

We see from this table that all the moduli, except $n = 244 = 2^2 \cdot 61$, have at least two distinct prime factors that are congruent to 1 modulo M. In fact, we have:

Theorem 2. *Let $M \geq 2$ be an integer, and suppose that the positive integer n has at least two distinct prime factors congruent to* $1 \pmod{M}$. *Then all the partial products $\Pi_j^{(M)}$ are congruent modulo n, that is, the congruences* (4.1) *hold.*

Our starting point for the proof of Theorem 2 is the observation that each partial product $\Pi_j^{(M)}$ can be written as a quotient of two Gauss factorials that are similar in nature. In particular, we see immediately from the definitions (2.5) and (2.2) that

$$\Pi_j^{(M)} = \frac{\left(j\frac{n-1}{M}\right)_n!}{\left((j-1)\frac{n-1}{M}\right)_n!}, \quad j = 1, 2, \dots, M, \tag{4.2}$$

with the convention that $0_n! = 1$. We therefore need to study the Gauss factorials on the right-hand side of (4.2). Our main tool is the following explicit congruence, obtained as a generalization of Proposition 2 in [**7**].

Lemma 2. *Let $M \geq 2$ and $n \equiv 1 \pmod{M}$, $n = p^\alpha q^\beta w$ for distinct prime $p, q \equiv 1 \pmod{M}$, $\alpha, \beta \geq 1$, and $\gcd(pq, w) = 1$. Then for $i = 1, 2, \ldots, M$ we have*

$$\left(i\tfrac{n-1}{M}\right)_n! \equiv \frac{\varepsilon^{i\frac{p-1}{M}}}{p^{iA}} \pmod{q^\beta w}, \quad A = \frac{p^{\alpha-1}}{M}\phi(q^\beta w), \tag{4.3}$$

where $\varepsilon = -1$ if $w = 1$, and $\varepsilon = 1$ if $w > 1$, and $\phi(m)$ denotes Euler's totient function.

Now, combining the congruence (4.3) with (4.2), we get

$$\Pi_j^{(M)} \equiv \frac{\varepsilon^{\frac{p-1}{M}}}{p^A} \pmod{q^\beta w}, \quad A = \frac{p^{\alpha-1}}{M}\phi(q^\beta w). \tag{4.4}$$

Since p^α and q^β are interchangeable, we also have

$$\Pi_j^{(M)} \equiv \frac{\varepsilon^{\frac{p-1}{M}}}{q^B} \pmod{p^\alpha w}, \quad B = \frac{q^{\beta-1}}{M}\phi(p^\alpha w). \tag{4.5}$$

By the Chinese remainder theorem, applied to (4.4) and (4.5), the partial product $\Pi_j^{(M)}$ is uniquely determined modulo $p^\alpha q^\beta w = n$, and most importantly, it is independent of j. This completes the proof of Theorem 2.

To prove Lemma 2, the main idea is to break the whole range of the product in the Gauss factorial $\left(i\frac{n-1}{M}\right)_n!$ into a number of products of approximately equal length and a shorter "tail." We then evaluate the products of the first type using the Gauss-Wilson theorem with modulus $\widetilde{n} := q^\beta w$. To do so we divide $i\frac{n-1}{M}$ by $\widetilde{n}$ with remainder:

$$i\frac{n-1}{M} = is\widetilde{n} + i\frac{\widetilde{n}-1}{M}, \quad \text{where} \quad s := \frac{p^\alpha - 1}{M}. \tag{4.6}$$

By hypothesis we know that s and $(\widetilde{n}-1)/M$ are both integers. Based on (4.6) we now decompose our Gauss factorial into is products of similar lengths and one shorter product; that is, we write

$$\left(i\tfrac{n-1}{M}\right)_n! = \left(\prod_{j=1}^{is} P_j\right) Q, \tag{4.7}$$

where

$$P_j := \prod_{\substack{k=1\\ \gcd((j-1)\widetilde{n}+k,n)=1}}^{\widetilde{n}-1} \big((j-1)\widetilde{n}+k\big), \quad Q := \prod_{\substack{k=1\\ \gcd(is\widetilde{n}+k,n)=1}}^{i\frac{\widetilde{n}-1}{M}} \big(is\widetilde{n}+k\big). \tag{4.8}$$

For a given j, if the set of residues $\{(j-1)\widetilde{n}+k \mid 1 \leq k \leq \widetilde{n}-1\}$, subject to $\gcd((j-1)\widetilde{n}+k, n) = 1$, formed a reduced residue system modulo $\widetilde{n}$, then the product P_j would, by the Gauss-Wilson theorem, be congruent to $-1 \pmod{\widetilde{n}}$ if $w = 1$, and to $1 \pmod{\widetilde{n}}$ if $w > 1$. However, this is not always the case because the residues that appear in the product $\left(i\frac{n-1}{M}\right)_n!$ have none divisible by p; these residues have been removed from the normal factorial $\left(i\frac{n-1}{M}\right)!$ in forming the corresponding Gauss factorial.

To deal with the variable nature of these P_j, we multiply all relevant multiples of p back into $P_1, \dots, P_{is}$, and into Q as well. Thus, on the right-hand side of (4.7) we multiply numerator and denominator by

$$\prod_{\substack{j=1 \\ \gcd(j,\widetilde{n})=1}}^{s'} jp, \tag{4.9}$$

where

$$s' = \frac{i}{M}\left(p^{\alpha-1}q^{\beta}w - 1\right),$$

which comes from the obvious division

$$i\frac{n-1}{M} = s'p + i\frac{p-1}{M}, \tag{4.10}$$

where s' and $\frac{p-1}{M}$ are integers, by hypothesis. To count the number of elements in the product (4.9), we do yet another obvious division, namely

$$\left(p^{\alpha-1}q^{\beta}w - 1\right) = \left(p^{\alpha-1} - 1\right)q^{\beta}w + \left(q^{\beta}w - 1\right),$$

giving

$$s' = \frac{i}{M}\left(p^{\alpha-1} - 1\right)\widetilde{n} + \frac{i}{M}(\widetilde{n} - 1). \tag{4.11}$$

Counting the number of elements in the product (4.9) for each of the intervals of length $\widetilde{n}$ is no problem; there are exactly $\phi(\widetilde{n})$ elements in each of these intervals. The only problem is to deal with the remainder term in (4.11), and for that we need Lemma 1. Using (4.11) and (3.2) with $\widetilde{n}$ in place of n, we see that the number of elements in the product (4.9) is

$$\frac{i}{M}\left(p^{\alpha-1} - 1\right)\phi(\widetilde{n}) + \frac{i}{M}\phi(\widetilde{n}) = \frac{i}{M}p^{\alpha-1}\phi(\widetilde{n}). \tag{4.12}$$

But this expression is iA, with A as defined in (4.3). We therefore get from (4.7),

$$\left(i\tfrac{n-1}{M}\right)_n! \equiv \frac{\overline{P_1}\cdots\overline{P_{is}}\cdot\overline{Q}}{p^{iA}\prod_{j=1,\gcd(j,\widetilde{n})=1}^{s'} j} \pmod{\widetilde{n}}. \tag{4.13}$$

Here the bars over the P_j and Q indicate that the products (4.8) are taken over *all* k relatively prime to $\widetilde{n}$, that is,

$$\overline{P_j} := \prod_{\substack{k=1 \\ \gcd(k,\widetilde{n})=1}}^{\widetilde{n}-1} \left((j-1)\widetilde{n} + k\right), \quad \overline{Q} := \prod_{\substack{k=1 \\ \gcd(k,\widetilde{n})=1}}^{i\frac{\widetilde{n}-1}{M}} \left(is\widetilde{n} + k\right).$$

But then the Gauss-Wilson theorem gives

$$\overline{P_1} \equiv \cdots \equiv \overline{P_{is}} \equiv \begin{cases} -1 \pmod{\widetilde{n}} & \text{if } w = 1, \\ 1 \pmod{\widetilde{n}} & \text{if } w > 1. \end{cases} \tag{4.14}$$

From the definition of $\overline{Q}$ we get

$$\overline{Q} \equiv \prod_{\substack{k=1\\ \gcd(k,\widetilde{n})=1}}^{i\frac{\widetilde{n}-1}{M}} (is\widetilde{n}+k) \equiv \prod_{\substack{k=1\\ \gcd(k,\widetilde{n})=1}}^{i\frac{\widetilde{n}-1}{M}} k \pmod{\widetilde{n}}. \tag{4.15}$$

The Gauss factorial in the denominator of (4.13) can be split up into $i\frac{p^{\alpha-1}-1}{M}$ products that are congruent to the $\overline{P_j}$ and a remainder that is congruent to $\overline{Q}$ (mod $\widetilde{n}$); this follows from (4.11). Hence (4.14) and (4.15) together with (4.13) give

$$\left(i\tfrac{n-1}{M}\right)_n! \equiv \frac{\varepsilon^B}{p^{iA}} \pmod{\widetilde{n}}, \tag{4.16}$$

with A defined by (4.12) and

$$B = is - i\frac{p^{\alpha-1}-1}{M} = i\frac{p^{\alpha}-1}{M} - i\frac{p^{\alpha-1}-1}{M} = ip^{\alpha-1}\frac{p-1}{M}.$$

Since p is odd, we have $\varepsilon^B = \varepsilon^{i\frac{p-1}{M}}$; this completes the proof of Lemma 2.

We conclude this section with the remark that Theorem 2 is best possible. Indeed, consider the example $M = 3$ and $n = 70 = 2 \cdot 5 \cdot 7$. Here 7 is the only prime factor of 70 that is congruent to 1 (mod 3), and Table 2 shows that $\Pi_1^{(3)} \not\equiv \Pi_2^{(3)}$ (mod n). This is similar to the observation, at the beginning of Section 3, that Lehmer's result is best possible.

On the other hand, while Theorem 2 gives a sufficient condition, this condition is not necessary, as we already saw in Table 4.

5. SOME CONSEQUENCES. We begin this brief section with an immediate consequence of Theorem 2. Let M and n be as in Theorem 2. Since the product of all partial products $\Pi_j^{(M)}$ for a fixed M is the Gauss factorial $(n-1)_n!$, the congruences (4.1) and the Gauss-Wilson theorem (2.1) give

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

This implies:

Corollary 1. *Let $M \geq 2$ be an integer, and suppose that the positive integer n has at least two distinct prime factors congruent to* 1 (mod M). *Then the multiplicative order of the Gauss factorial $(\frac{n-1}{M})_n!$ modulo n is a divisor of M.*

While in Lemma 2 the factor w plays only an auxiliary role, collecting all the irrelevant prime powers in n (if any), it turns out that we obtain some interesting results if we consider the Gauss factorial in (4.3) modulo w. Indeed, using the multiplicativity of $\phi(n)$ and the fact that M divides $q-1$, we can rewrite A in (4.3) as

$$A = \frac{p^{\alpha-1}}{M}\phi(q^{\beta})\phi(w) = p^{\alpha-1}\frac{(q-1)q^{\beta-1}}{M}\phi(w) = C\phi(w)$$

for some integer C. Then, since $p \nmid w$, we can apply Euler's generalization of Fermat's little theorem and obtain

$$p^{iA} = \left(p^{iC}\right)^{\phi(w)} \equiv 1 \pmod{w}.$$

If $w > 1$ then $\varepsilon = 1$, and the numerator in the congruence in (4.3) is 1. We therefore get the following corollary.

Corollary 2. *Let M, n, and w be as in Lemma 2. Then for $i = 1, 2, \dots, M$ we have*

$$\left(i\tfrac{n-1}{M}\right)_n! \equiv 1 \pmod{w} \quad \textit{and} \quad \Pi_i^{(M)} \equiv 1 \pmod{w}. \tag{5.1}$$

This holds for $w = 1$ because in that case the congruences are trivially true. As a further consequence we obtain the following result, a special case of which was already proven as Proposition 4 in [**7**]. We formulate it as a theorem since it supplements Theorem 2.

Theorem 3. *Let $M \geq 2$ be an integer, and suppose that the positive integer n has at least three distinct prime factors congruent to $1 \pmod{M}$. Then*

$$\Pi_i^{(M)} \equiv 1 \pmod{n} \quad \textit{for} \quad i = 1, 2, \dots, M. \tag{5.2}$$

To prove this result, we write $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}\overline{w}$, where p_1, p_2, p_3 are distinct primes with $p_j \equiv 1 \pmod{M}$, $\alpha_j \geq 1$ for $j = 1, 2, 3$, and $\gcd(p_1p_2p_3, \overline{w}) = 1$. Now we apply Corollary 2 with w replaced by $w_j := p_j^{\alpha_j}\overline{w}$, $j = 1, 2, 3$, obtaining $\Pi_i^{(M)} \equiv 1 \pmod{w_j}$ for $j = 1, 2, 3$. The congruences (5.2) then follow immediately from the Chinese remainder theorem.

In [**7**] it was shown by similar methods that $(\frac{n-1}{M})_n! = \Pi_1^{(M)} \equiv 1 \pmod{n}$ under the conditions of Theorem 3. It was also shown by way of an example that this result, and thus Theorem 3, is best possible: Let $M = 3$ and $n = 2^2 \cdot 7 \cdot 13 = 364$. Then obviously $364 \equiv 7 \equiv 13 \equiv 1 \pmod{3}$, and it is easy to compute $(\frac{n-1}{3})_n! = 121_{364}! \equiv 113 \pmod{364}$.

In analogy to the example at the end of the previous section we show that the condition in Theorem 3 is not necessary. Let $M = 12$ and consider $n = 146965 = 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19$. Then only one prime factor of n is congruent to 1 modulo M, but $\Pi_j^{(12)} \equiv 1 \pmod{n}$ for all j.

6. THE GAUSS AND JACOBI BINOMIAL COEFFICIENT THEOREMS.

In Section 1 we remarked in connection with Table 1 that there are no obvious relationships between $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$. One way to explore this further is to consider the quotient of these partial products. Now, by (1.6) it is clear that for $p \equiv 1 \pmod{4}$, $\Pi_1^{(4)} = \frac{p-1}{4}!$ and $\Pi_1^{(4)}\Pi_2^{(4)} = \frac{p-1}{2}!$, and therefore

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}} = \frac{\Pi_1^{(4)}\Pi_2^{(4)}}{\left(\Pi_1^{(4)}\right)^2} = \frac{\frac{p-1}{2}!}{\left(\frac{p-1}{4}!\right)^2} = \binom{\frac{p-1}{2}}{\frac{p-1}{4}}. \tag{6.1}$$

Table 5 lists the values of $Q_4(p) \pmod{p}$ for all the appropriate primes $p < 100$, where both the least positive and the least absolute residues are given.

While the least positive residues do not perhaps reveal much, we see a strong connection between the least absolute residues and the representation of p as a sum of two squares, the existence and uniqueness of which are guaranteed by the well-known two-squares theorem of Fermat. Even the sign pattern is now quite obvious: the least absolute residue is positive if and only if $a \equiv 1 \pmod{4}$.

Table 5. $Q_4(p)$ (mod p) for $p \equiv 1 \pmod 4$, $p < 100$, and a, b for which $p = a^2 + b^2$, with a odd.

p	least pos. res.	least abs. res.	a	b
5	2	2	1	2
13	7	−6	3	2
17	2	2	1	4
29	10	10	5	2
37	2	2	1	6
41	10	10	5	4
53	39	−14	7	2
61	10	10	5	6
73	67	−6	3	8
89	10	10	5	8
97	18	18	9	4

All this is in fact explained by the following celebrated theorem of Gauss. We fix p, a, and b such that

$$p \equiv 1 \pmod 4, \quad p = a^2 + b^2, \quad a \equiv 1 \pmod 4. \tag{6.2}$$

Gauss's binomial coefficient theorem of 1828 can now be stated as follows.

Theorem 4 (Gauss). *Let the prime p and the integer a be as in* (6.2). *Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p. \tag{6.3}$$

As a first easy application of this theorem we show that

$$\Pi_2^{(4)} \not\equiv \pm\Pi_1^{(4)} \pmod p \quad \text{for all} \quad p \equiv 1 \pmod 4.$$

Indeed, if this were not the case, then $Q_4(p) \equiv \pm 1 \pmod p$. But by (6.1) and (6.3) we have $Q_4(p) \equiv 2a \pmod p$, so that $2a \equiv \pm 1 \pmod p$. The smallest possible solutions of this congruence are $a = \pm\frac{p-1}{2}$. However, by (6.2) we have $|a| < \sqrt{p}$, but also $\sqrt{p} < \frac{p-1}{2}$ for $p > 5$. This means that there are no solutions, which was to be shown. (The case $p = 5$ is clear from Table 1.)

The analogous investigation for the case $M = 3$ is a bit more involved, which is why we present it second. For primes $p \equiv 1 \pmod 6$ we begin, in analogy to (6.1), by considering

$$Q_3(p) := \frac{\Pi_2^{(3)}}{\Pi_1^{(3)}} = \frac{\Pi_1^{(3)}\Pi_2^{(3)}}{\left(\Pi_1^{(3)}\right)^2} = \frac{(2\frac{p-1}{3})!}{(\frac{p-1}{3}!)^2} = \binom{2\frac{p-1}{3}}{\frac{p-1}{3}}. \tag{6.4}$$

In an attempt to find a congruence for $Q_3(p)$ that is analogous to (6.3) one might want to try another two-squares formula of Fermat, namely $p = a^2 + 3b^2$ for primes $p \equiv 1$ (mod 6), which is unique up to signs. (For the early history of such representations, see [**15**, pp. 14ff.].) However, as columns 2 and 3 of Table 6 show, there seems to be no apparent relationship modulo p between $Q_3(p)$ and a or b.

It was Jacobi who, in 1837, used instead the representation $4p = x^2 + 3y^2$, which always has three distinct solutions, namely $(|2a|, |2b|)$, $(|a + 3b|, |a - b|)$, and $(|a -$

Table 6. $Q_3(p)$ (mod p) for $p \equiv 1$ (mod 6), $p < 100$, and the solutions of $p = a^2 + 3b^2$, $4p = x^2 + 3y^2$.

p	$Q_3(p)$ (mod p)	a, b	x_1, y_1	x_2, y_2	x_1, y_1	r, s
7	-1	2, 1	5, 1	4, 2	1, 3	1, 3
13	5	1, 2	7, 1	5, 3	2, 4	−5,3
19	-7	4, 1	8, 2	7, 3	1, 5	7, 3
31	-4	2, 3	11, 1	7, 5	4, 6	4, 6
37	11	5, 2	11, 3	10, 4	1, 7	−11, 3
43	8	4, 3	13, 1	8, 6	5, 7	−8, 6
61	-1	7, 2	14, 4	13, 5	1, 9	1, 9
67	5	8, 1	16, 2	11, 7	5, 9	−5, 9
73	-7	5, 4	17, 1	10, 8	7, 9	7, 9
79	17	2, 5	17, 3	13, 7	4, 10	−17, 3
97	-19	7, 4	19, 3	14, 8	5, 11	19, 3

$3b|$, $|a+b|$). These three solutions, for $p < 100$, are listed in columns 4–6 of Table 6. One of these solutions always satisfies $y \equiv 0 \pmod 3$; it is then the corresponding x, with its sign appropriately chosen, that gives the desired congruence. To be exact, suppose that the prime p and integers r, s are such that

$$p \equiv 1 \pmod 6, \quad 4p = r^2 + 3s^2, \quad r \equiv 1 \pmod 3, \quad s \equiv 0 \pmod 3. \tag{6.5}$$

The integer r is then uniquely determined, and we can now state Jacobi's binomial coefficient theorem, which is illustrated in the last column of Table 6.

Theorem 5 (Jacobi). *Let p and r be as in* (6.5). *Then*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p. \tag{6.6}$$

Proofs of the theorems of Gauss and Jacobi are nonelementary and can be found in the book [**2**] by Berndt, Evans, and Williams, which is the standard reference in the field. For remarks and references, see [**2**, p. 291]. It is worth giving an explicit connection between the a in $p = a^2 + 3b^2$, with its sign fixed by the condition $a \equiv -1 \pmod 3$, and the r as fixed in (6.5):

$$r = \begin{cases} 2a & \text{if} \quad b \equiv 0 \pmod 3, \\ -(a - 3b) & \text{if} \quad b \equiv 1 \pmod 3, \\ -(a + 3b) & \text{if} \quad b \equiv 2 \pmod 3. \end{cases}$$

This is an easily obtained modification of congruences in [**2**, p. 269].

Returning to our observations in Section 1, we now use Jacobi's theorem to show that

$$\Pi_2^{(3)} \not\equiv \Pi_1^{(3)} \pmod p \quad \text{for all} \quad p \equiv 1 \pmod 6.$$

Indeed, if this were not the case, we would have $r \equiv -1 \pmod p$ by (6.4) and (6.6). Now $r = -1$ is impossible since $r \equiv 1 \pmod 3$. The next smallest solution, $r = p - 1$, is also impossible since by (6.5) we have $|r| < 2\sqrt{p}$, but we already saw that $2\sqrt{p} < p - 1$ for $p > 5$.

Now we turn to the congruence $\Pi_2^{(3)} \equiv -\Pi_1^{(3)} \pmod{p}$ which, as we saw in Table 1, does have solutions. Again by (6.4) and (6.6), the congruence is equivalent to $r \equiv 1 \pmod{p}$. This time we have the solution $r = 1$, but by the same size argument as above, there are no others, and (6.5) gives $4p = 1 + 3s^2$. Now $s \equiv 0 \pmod{3}$ and it also has to be odd, which means that $s = 6x + 3$ for some positive integer x. If we substitute this into the expression for $4p$, we get the following result.

Corollary 3. *For a prime $p \equiv 1 \pmod{6}$ we have $\Pi_2^{(3)} \equiv -\Pi_1^{(3)} \pmod{p}$ if and only if $p = 27x^2 + 27x + 7$ for an integer x.*

The first primes generated by this formula are 7, 61 (see Table 1), 331, 547, and 1951. As is easily seen, negative x give rise to the same primes. It is, of course, not known whether there are infinitely many primes of this form.

We continue this section with some remarks on congruences for the factorials $\frac{p-1}{4}!$ and $\frac{p-1}{3}!$, all of which follow from the theorems of Gauss and Jacobi, respectively.

First, consider primes of the form $p \equiv 1 \pmod{4}$. Then

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

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

(c) $\left(\frac{p-1}{4}!\right)^8 \equiv -1 \pmod{p}$ does hold for $p = 17, 241, 3361, 46817, 652081, \dots$

For primes of the form $p \equiv 1 \pmod{6}$ we have

(d) $\frac{p-1}{3}! \equiv 1 \pmod{p}$ holds for $p = 3571, 4219, 13669, 25117, 55897, \dots$

(e) $\left(\frac{p-1}{3}!\right)^3 \equiv 1 \pmod{p}$ holds if and only if $p = 27x^2 + 27x + 7$ for some integer x.

(f) $\left(\frac{p-1}{3}!\right)^9 \equiv 1 \pmod{p}$ holds if and only if $p = 3y^2 + 3y + 1$ for some integer y. Furthermore, the multiplicative order of $\frac{p-1}{3}! \pmod{p}$ is 9 if and only if p is of the form $p = 27x^2 + 9x + 1$ or $p = 27x^2 + 45x + 19$.

(g) $\left(\frac{p-1}{3}!\right)^k \not\equiv -1 \pmod{p}$ for $k = 1, 3, 9$.

(h) $\left(\frac{p-1}{3}!\right)^{18} \equiv -1 \pmod{p}$ holds if and only if p satisfies $p^2 = 3y^2 + 3y + 1$ for some integer y. The first few such primes are 13, 181, 2251, 489061.

Statements (c) and (h) are actually connected in the following surprising way: The identity for p^2 in (h) can be rewritten in the form of the Pell equation $(2p)^2 - 3(2y + 1)^2 = 1$. The infinitely many solutions (A_n, B_n) of the equation $A^2 - 3B^2 = 1$ are given by the recurrence relations (see, e.g., [**25**, p. 354])

$$A_{n+2} = 4A_{n+1} - A_n, \qquad A_0 = 1, A_1 = 2,$$
$$B_{n+2} = 4B_{n+1} - B_n, \qquad B_0 = 0, B_1 = 1.$$

Then, as is shown in [**9**], the primes p in (h) are given by primes $\frac{1}{2}A_{2k-1}$, while those in (c) are given by prime values of $B_{n-1}^2 + B_n^2$.

While details concerning (h) can be found in [**9**], statements (a)–(g) are derived and further discussed in a forthcoming paper [**10**]. However, some of them follow immediately from results earlier in this section. For instance, if we square (6.1) and use the fact that by (1.3) we have $(\frac{p-1}{2}!)^2 \equiv -1 \pmod{p}$, then we get $(\frac{p-1}{4}!)^4 \equiv -Q_4(p)^{-2} \pmod{p}$. Since we know that $Q_4(p) \not\equiv -1 \pmod{p}$, this proves statement (b) for $k = 4$. The solutions in statement (c) are related to a certain Pell equation; see [**4**,

p. 318]. These primes form a subsequence of the sequence of all integers a with the property that a triangle with integer sides $(a, a, a-1)$ has integer area; see [**28**, A103772].

For primes $p \equiv 1 \pmod 6$ we use (1.5) and (1.1) to rewrite (6.4) as

$$Q_3(p) = \frac{\Pi_1^{(3)}\Pi_2^{(3)}\Pi_3^{(3)}}{(\Pi_1^{(3)})^3} \equiv -\left(\tfrac{p-1}{3}!\right)^{-3} \pmod p. \tag{6.7}$$

We have seen that $Q_3(p) \equiv 1 \pmod p$ is impossible, which proves statement (g) for $k = 3$ and also for $k = 1$. On the other hand, the case $Q_3(p) \equiv -1 \pmod p$ is equivalent to Corollary 3; hence (6.7) gives statement (e). A proof along these lines was suggested by Andrew Granville (private communication with the first author, December, 2004); see also [**6**].

Statement (e) means that the multiplicative order of $\frac{p-1}{3}!$ modulo p is 1 or 3 when $p = 27x^2 + 27x + 7$ for some integer x. Order 1 does actually occur, as statement (d) indicates. Computations that were kindly carried out for us by Yves Gallot show that there are 364 such primes up to 10^9, while for 762 primes up to 10^9 the order of $\frac{p-1}{3}!$ is 3. It appears to be a difficult question to find a criterion for when the order is 1 and when it is 3. Also, the data suggest that the split between these two classes may approach 1:2.

Returning to statement (e) and Corollary 3, recall that the polynomial expression for p comes from

$$4p = 1 + 3s^2 = 1 + 3(2y+1)^2, \quad \text{or} \quad p = 3y^2 + 3y + 1 = (y+1)^3 - y^3, \tag{6.8}$$

where we have put $s = 2y + 1$ since s has to be odd. Now Jacobi's theorem required $3 \mid s$, that is, $y = 3x + 1$, which led to $p = 27x^2 + 27x + 7$. In the other two cases, namely $y = 3x$ and $y = 3x + 2$, we get $p = 27x^2 + 9x + 1$ and $p = 27x^2 + 45x + 19$, respectively. In both these cases the order of $\frac{p-1}{3}!$ is 9, as is shown in [**10**]. This, together with (6.8), gives statement (f).

To conclude this section we note that for Gauss factorials with *composite* moduli the situation related to statements (a) and (d) is very different: As Theorem 3 shows, for each $M \geq 2$ we have $(\frac{n-1}{M})_n! \equiv 1 \pmod n$ for infinitely many n, namely all those with at least three distinct prime factors $p \equiv 1 \pmod M$.

However, if these composite moduli are prime powers, then the situation remains very interesting. In fact, in [**9**] we showed that for a given $M \geq 2$ and $p \equiv 1 \pmod M$ the sequence of multiplicative orders mod p^α of the Gauss factorials

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

almost always depends in a predictable way on the order of $\frac{p-1}{M}!$ modulo p. However, there are some exceptional primes, depending on M, which leads to further interesting phenomena, mostly explained in [**9**]. In the case $M = 3$ this is in fact related to our remark following statement (h) above.

7. EXTENSIONS OF THE GAUSS BINOMIAL COEFFICIENT THEOREM.

In most of the first five sections of this paper we have dealt with Gauss factorials and the related products $\Pi_j^{(M)}$ for composite moduli, often with at least two distinct prime factors. The case of moduli with only *one* prime factor, namely prime powers, turns out to be the most interesting and deepest case in spite of its apparent simplicity. An indication of this was already provided by the theorems of Gauss and Jacobi in the previous section, and in the remark at the very end of that section. In the present section we will describe a further instance of the depth of the prime power case.

In attempting to extend or generalize the theorems of Gauss and Jacobi one might take two different approaches: First, a natural question is to ask about congruences modulo p^2 for the binomial coefficients $\binom{(p-1)/2}{(p-1)/4}$ and $\binom{2(p-1)/3}{(p-1)/3}$, thus extending the modulo p congruences of the classical theorems. This was indeed done, as we will see shortly.

A second approach, natural from the point of view of Gauss factorials, is to consider the relevant binomial coefficients in terms of factorials. Then one can extend these objects to Gauss factorials with *composite* moduli n, and consider the corresponding quotients modulo n. It turns out that the most interesting case is that of prime power moduli, which is then related to the first approach, but from a different point of view.

Returning to this first approach, the following extension of the theorem of Gauss to modulus p^2 was first conjectured by Beukers [**3**], and later proved by Chowla, Dwork, and Evans [**5**].

Theorem 6 (Chowla, Dwork, Evans). *Let p and a be as in* (6.2). *Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \left(1+\frac{1}{2}pq_p(2)\right)\left(2a-\frac{p}{2a}\right) \pmod{p^2}, \tag{7.1}$$

where $q_p(2) := (2^{p-1}-1)/p$ is the Fermat quotient to base 2.

Congruences such as (7.1) have been very useful in large-scale computations to search for Wilson primes, that is, primes p satisfying the congruence $(p-1)! \equiv -1 \pmod{p^2}$; see [**11**] or [**12**]. For a proof of (7.1) and generalizations to numerous other binomial coefficients, see [**2**].

Turning now to the Gauss factorial approach, the analogue of $\binom{(p-1)/2}{(p-1)/4} \pmod{p}$, with modulus $n = p^\alpha$, is

$$B^{(\alpha)}(p) := \frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2} \pmod{p^\alpha}. \tag{7.2}$$

Obviously $\alpha = 1$ gives the usual binomial coefficient. For $\alpha = 2$ we were able to show that the congruence (7.1) is equivalent to

$$B^{(2)}(p) \equiv 2a - \frac{p}{2a} \pmod{p^2}. \tag{7.3}$$

Seeing the simplicity of (7.3) as compared with (7.1), one is led to search numerically for congruences modulo higher powers of p. Indeed, one readily conjectures that

$$B^{(3)}(p) \equiv 2a - \frac{p}{2a} - \frac{p^2}{8a^3} \pmod{p^3}. \tag{7.4}$$

Continuing with higher powers, we were then able to conjecture and ultimately prove:

Theorem 7. *Let p and a be as in* (6.2) *and let $\alpha \geq 2$ be an integer. Then*

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

$$= 2a - 2a\sum_{j=1}^{\alpha-1}\frac{1}{j}\binom{2j-2}{j-1}\left(\frac{p}{4a^2}\right)^j \pmod{p^\alpha}, \tag{7.5}$$

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

The first few Catalan numbers $C_0, C_1, \ldots$ are 1, 1, 2, 5, 14, 42, 132, ... The proof of Theorem 7 uses methods similar to those in the proof of Theorem 6; see [**2**, Theorem 9.4.3]. The Catalan numbers enter through certain combinatorial identities that are related to αth powers of particular binomial expressions in complex numbers. For details, see [**8**].

If the summation on the right of (7.5) is considered 0 for $\alpha = 1$, then Gauss's Theorem 4 can be seen as a special case of (7.5). We already remarked that for $\alpha = 2$ the congruences (7.5) and (7.1) are equivalent. This leads to the natural question of whether one can derive a binomial coefficient analogue to (7.5) for $\alpha = 3$. This is in fact possible, and we obtain the following mod p^3 extension of Theorem 6.

Theorem 8. *Let p and a be as in* (6.2). *Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \left(2a - \frac{p}{2a} - \frac{p^2}{8a^3}\right)$$

$$\times \left(1 + \tfrac{1}{2}pq_p(2) + \tfrac{1}{8}p^2\left(2E_{p-3} - q_p(2)^2\right)\right) \pmod{p^3}, \tag{7.6}$$

where E_n is the nth Euler number.

For further details and proofs, see [**8**], where Jacobi's Theorem 5 has also been extended in a similar fashion.

To summarize: Comparing the congruences (7.5) and (7.6), it is clear that for higher congruences the Gauss factorials with prime power moduli are the more natural objects to study than the usual factorials.

8. CONCLUSION.

The number-theoretic object we propose to call a *Gauss factorial* is certainly not new. For instance, it has played an important role in the study of arithmetic properties of binomial coefficients [**18**], and is essential in the definition of Morita's p-adic gamma function (see, e.g., [**2**, p. 277]). This paper, however, is a study of Gauss factorials as objects in their own right. In this study, we relied heavily on numerical experimentation using the computer algebra system Maple. In fact, without the assistance of such a tool this study would not have been possible.

Our purpose in this paper has been threefold: First, to study the special Gauss factorials $(\frac{n-1}{M})_n!$, and in particular their values and multiplicative orders modulo n, in the spirit of the remarkable but little-known Gauss-Wilson theorem, which is the special case $M = 1$.

The second purpose has been the introduction and study of the associated partial products $\Pi_j^{(M)}$, defined by (2.5), which extend the Gauss factorials since $\Pi_1^{(M)} =$

$(\frac{n-1}{M})_n!$. Our main results, Theorems 2 and 3, are different in nature from most results in classical number theory in that they depend on the number of different prime factors of a given n. The only result of this nature of which we are aware is that of D. H. Lehmer (Lemma 1); our results complement his in that they concern the *products* of "totatives," as opposed to their numbers.

Our third purpose has been to show that some deep extensions of the binomial theorems of Gauss and Jacobi appear in a simpler and more natural way, and can be further extended, if stated in terms of Gauss factorials. This also points to the fact that Gauss factorials are particularly worthwhile objects to study when the modulus n is a power of an odd prime.

In summary, we hope that we have demonstrated the inherent beauty, depth, and usefulness of Gauss factorials.

ACKNOWLEDGMENTS. We would like to thank Yves Gallot for generously carrying out the computations reported in Section 6. We also thank Andrew Granville for suggesting the proof mentioned in Section 6.

REFERENCES

1. T. Agoh, K. Dilcher, and L. Skula, Wilson quotients for composite moduli, *Math. Comp.* **67** (1998) 843–861. http://dx.doi.org/10.1090/S0025-5718-98-00951-X
2. B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.
3. F. Beukers, Arithmetical properties of Picard-Fuchs equations, in *Seminar on Number Theory—Paris, 1982–83*, Progr. Math., vol. 51, M.-J. Bertin and C. Goldstein, eds., Birkhäuser, Boston, MA, 1984, 33–38.
4. J. M. Borwein and D. Bailey, *Mathematics by Experiment. Plausible Reasoning in the 21st Century*, 2nd ed., A K Peters, 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) 188–196. http://dx.doi.org/10.1016/0022-314X(86)90102-2
6. J. B. Cosgrave, Trinity College Dublin Mathematical Society Lecture, available at http://staff.spd.dcu.ie/johnbcos/jacobi.htm.
7. 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.
8. ———, Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients, *Acta Arith.* **142** (2010) 103–118. http://dx.doi.org/10.4064/aa142-2-1
9. ———, The multiplicative orders of certain Gauss factorials, *Int. J. Number Theory* **7** (2011) 145–171. http://dx.doi.org/10.1142/S179304211100396X
10. ———, The Gauss-Wilson theorem for one-third, one-quarter and one-sixth intervals (in preparation).
11. R. Crandall, *Topics in Advanced Scientific Computation*, Springer-Verlag, New York, 1996.
12. R. E. Crandall, K. Dilcher, and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* **66** (1997) 433–449. http://dx.doi.org/10.1090/S0025-5718-97-00791-6
13. L. E. Dickson, *History of the Theory of Numbers. Volume I: Divisibility and Primality*, Chelsea, New York, 1966.
14. P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, 4th ed., ed. and supplemented by R. Dedekind, Chelsea, New York, 1968; translated as *Lectures on Number Theory* by J. Stillwell, American Mathematical Society, Providence, RI, 1999.
15. H. M. Edwards, *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, New York, 1977.
16. P. Erdős, Some remarks on a paper of McCarthy, *Canad. Math. Bull.* **1** (1958) 71–75. http://dx.doi.org/10.4153/CMB-1958-008-7
17. C. F. Gauss, *Disquisitiones Arithmeticae* (trans. and preface by A. A. Clarke), Yale University Press, New Haven, 1966; rev. by W. C. Waterhouse, C. Greither, and A. W. Grootendorst with preface by W. C. Waterhouse, Springer-Verlag, New York, 1986.
18. A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, in *Organic Mathematics—Burnaby, BC, 1995*, CMS Conf. Proc., vol. 20, American Mathematical Society, Providence, RI, 1997, 253–276.
19. R. R. Hall and P. Shiu, The distribution of totatives, *Canad. Math. Bull.* **45** (2002) 109–114. http://dx.doi.org/10.4153/CMB-2002-012-1

20. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, New York, 1979.
21. P. Kesava Menon, A generalization of Wilson's theorem, *J. Indian Math. Soc. (N.S.)* **9** (1945) 79–88.
22. K. E. Kloss, Some number theoretic calculations, *J. Res. Nat. Bureau of Stand. B* **69** (1965) 335–339.
23. D. H. Lehmer, The distribution of totatives, *Canad. J. Math.* **7** (1955) 347–357. http://dx.doi.org/10.4153/CJM-1955-038-5
24. L. J. Mordell, The congruence $(p-1/2)! \equiv \pm 1 \pmod{p}$, *Amer. Math. Monthly* **68** (1961) 145–146. http://dx.doi.org/10.2307/2312481
25. I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, New York, 1991.
26. S. Sanielevici, Une généralisation du théorème de Wilson, *Com. Acad. R. P. Romîne* **8** (1958) 737–744.
27. Š. Schwarz, The role of semigroups in the elementary theory of numbers, *Math. Slovaca* **31** (1981) 369–395.
28. N. J. A. Sloane, *On-Line Encyclopedia of Integer Sequences*, available at http//oeis.org/.

JOHN B. COSGRAVE was born in Bailieboro, County Cavan, Ireland. He received his B.Sc. (1968) and Ph.D. (1972) in Mathematics from Royal Holloway College (London University). He worked at RHC, Manchester, Jos (Nigeria), Carysfort College (Dublin), and finally St. Patrick's College, Drumcondra, Dublin, where—shortly before retiring in 2007—he had the pleasure of having Doron Zeilberger as his department's international external assessor. Besides elementary number theory, his interests include reading (all kinds), music, and cycling, and—together with his wife Mary, whom he met at RHC—he is a daily swimmer in Dublin Bay.
79 Rowanbyrn, Blackrock, County Dublin, Ireland
jbcosgrave@gmail.com
http://staff.spd.dcu.ie/johnbcos/

KARL DILCHER received his undergraduate education at the Technische Universität Clausthal in Germany. He then did his graduate studies at Queen's University in Kingston, Ontario, and finished his Ph.D. there in 1983 under the supervision of Paulo Ribenboim. He is currently a professor at Dalhousie University in Halifax, Nova Scotia, Canada, where he first arrived in 1984 as a postdoctoral fellow. His research interests include classical analysis, special functions, and elementary and computational number theory.
Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 4R2, Canada
dilcher@mathstat.dal.ca