INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A39

EXTENSIONS OF THE GAUSS-WILSON THEOREM

John B. Cosgrave[1]
79 Rowanbyrn, Blackrock, County Dublin, Ireland
jbcosgrave@gmail.com

Karl Dilcher[2]
Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada
dilcher@mathstat.dal.ca

Received: 9/29/07, Revised: 8/22/08, Accepted: 8/25/08, Published: 9/17/08

Abstract

A theorem of Gauss extending Wilson's theorem states the congruence $(n-1)_n! \equiv -1 \pmod{n}$ whenever n has a primitive root, and $\equiv 1 \pmod{n}$ otherwise, where $N_n!$ denotes the product of all integers up to N that are relatively prime to n. In the spirit of this theorem we give a complete characterization of the multiplicative orders of $\left(\frac{n-1}{2}\right)_n! \pmod{n}$ for odd n. In most cases we are also able to evaluate this expression explicitly $\pmod{n}$, and some partial results extend to the more general case $\left(\frac{n-1}{M}\right)_n!$ for integers $M \geq 2$.

1. Introduction

One of the best-known and most important results in elementary number theory is Wilson's theorem and its converse by Lagrange, stating that p is a prime if and only if

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

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

Somewhat less well-known is Gauss' generalization of Wilson's theorem. In order to state it concisely, we introduce the following notation: For positive integers N and n let $N_n!$ denote

[1]Research supported by the Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography, Science Foundation Ireland Grant 06/MI/006
[2]Supported in part by the Natural Sciences and Engineering Research Council of Canada

the product of all integers up to N that are relatively prime to n, i.e.,

$$N_n! = \prod_{\substack{1\le j\le N\\ \gcd(j,n)=1}} j. \tag{2}$$

This notation is a slight variation of the one used in [8], 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 the theorem of Gauss, which can be stated as follows.

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

$$(n-1)_n! \equiv \begin{cases} -1 \pmod n & \text{for} \quad n = 2, 4, p^\alpha, \text{ or } 2p^\alpha, \\ 1 \pmod n & \text{otherwise}, \end{cases} \tag{3}$$

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

The first case of (3) indicates exactly those n that have primitive roots. For references, see [5, p. 65].

If we write out the factorial $(p-1)!$ and exploit symmetry modulo p, we obtain

$$1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2}\tfrac{p+1}{2} \cdot \ldots \cdot (p-1) \equiv \left(\tfrac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)! \pmod p, \tag{4}$$

and thus, with (1),

$$\left(\tfrac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p. \tag{5}$$

This was apparently first observed by Lagrange (see [5, p. 275]). Since for $p \equiv 1 \pmod 4$ the right-hand side of (5) is -1, we have immediately

$$\operatorname{ord}_p\left(\left(\tfrac{p-1}{2}\right)!\right) = 4 \quad \text{for} \quad p \equiv 1 \pmod 4, \tag{6}$$

where $\operatorname{ord}_p(a)$ denotes the multiplicative order of a modulo p. In the case $p \equiv 3 \pmod 4$ the congruence (5) gives

$$\left(\tfrac{p-1}{2}\right)! \equiv \pm 1 \pmod p, \tag{7}$$

and it turns out that determining the sign on the right-hand side is rather non-trivial. In fact, it was proved by Mordell [14] that for an odd prime $p \equiv 3 \pmod 4$ and $p > 3$,

$$\left(\tfrac{p-1}{2}\right)! \equiv -1 \pmod p \quad \Leftrightarrow \quad h(-p) \equiv 1 \pmod 4, \tag{8}$$

where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$. See also Remark 4 in Section 7 below.

In summary, the multiplicative order $\pmod p$ of $\left(\tfrac{p-1}{2}\right)!$ is completely determined as follows.

Corollary 1. *For any odd prime p we have*

$$\operatorname{ord}_p\left(\left(\tfrac{p-1}{2}\right)!\right) = \begin{cases} 4 & \text{if} \quad p \equiv 1 \pmod 4, \\ 2 & \text{if} \quad p \equiv 3 \pmod 4,\ p > 3,\ \text{and } h(-p) \equiv 1 \pmod 4, \\ 1 & \text{otherwise.} \end{cases} \tag{9}$$

For explicit values of $\left(\frac{p-1}{2}\right)!$, see Section 7.5 below. It is the purpose of this paper to extend (9) to arbitrary (composite but odd) moduli, in the spirit of Gauss' Theorem 1, which we shall also refer to as the Gauss-Wilson theorem.

It appears from Table 1 that just as in the prime case (9) the order of the Gauss factorial is at most 4, and is just 1 or 2 in most cases. This is indeed the case, as indicated by our main result.

n	factored	$a(n)$	$a(n)^2$	n	factored	$a(n)$	$a(n)^2$
9	3^2	-1	1	111	$3 \cdot 37$	-38	1
15	$3 \cdot 5$	-4	1	115	$5 \cdot 23$	-24	1
21	$3 \cdot 7$	8	1	117	$3^2 \cdot 13$	-53	1
25	5^2	7	-1	119	$7 \cdot 17$	-50	1
27	3^3	1	1	121	11^2	1	1
33	$3 \cdot 11$	10	1	123	$3 \cdot 41$	-40	1
35	$5 \cdot 7$	6	1	125	5^3	57	-1
39	$3 \cdot 13$	-14	1	129	$3 \cdot 43$	44	1
45	$3^2 \cdot 5$	-19	1	133	$7 \cdot 19$	-20	1
49	7^2	1	1	135	$3^3 \cdot 5$	26	1
51	$3 \cdot 17$	-16	1	141	$3 \cdot 47$	46	1
55	$5 \cdot 11$	-21	1	143	$11 \cdot 13$	-12	1
57	$3 \cdot 19$	20	1	145	$5 \cdot 29$	1	1
63	$3^2 \cdot 7$	8	1	147	$3 \cdot 7^2$	50	1
65	$5 \cdot 13$	-1	1	153	$3^2 \cdot 17$	35	1
69	$3 \cdot 23$	22	1	155	$5 \cdot 31$	-61	1
75	$3 \cdot 5^2$	26	1	159	$3 \cdot 53$	-52	1
77	$7 \cdot 11$	34	1	161	$7 \cdot 23$	-22	1
81	3^4	-1	1	165	$3 \cdot 5 \cdot 11$	1	1
85	$5 \cdot 17$	-1	1	169	13^2	70	-1
91	$7 \cdot 13$	27	1	171	$3^2 \cdot 19$	-37	1
93	$3 \cdot 31$	32	1	175	$5^2 \cdot 7$	76	1
95	$5 \cdot 19$	39	1	177	$3 \cdot 59$	58	1
99	$3^2 \cdot 11$	10	1	183	$3 \cdot 61$	-62	1
105	$3 \cdot 5 \cdot 7$	1	1	187	$11 \cdot 17$	-67	1

Table 1: $a(n) \equiv \left(\frac{n-1}{2}\right)_n! \pmod n$ for the first 50 odd composite n.

Theorem 2. *Let $n \geq 3$ be an odd integer, p and q distinct odd primes, and α, β positive integers. Then*

(1) $\operatorname{ord}_n\big((\frac{n-1}{2})_n!\big) = 4$ *when* $n = p^\alpha$ *and* $p \equiv 1 \pmod 4$*;*

(2) $\operatorname{ord}_n\big((\frac{n-1}{2})_n!\big) = 2$ *when*

(a) $n = p^{2\alpha-1}$, $p \equiv 3 \pmod 4$, $p > 3$, *and* $h(-p) \equiv 1 \pmod 4$, *or*

(b) $n = p^{2\alpha}$, $p = 3$, *or* $p \equiv 3 \pmod 4$ *and* $h(-p) \not\equiv 1 \pmod 4$, *or*

(c) $n = p^\alpha q^\beta$, $p \equiv q \equiv 1 \pmod 4$, *and* p *is a quadratic nonresidue* $\pmod q$, *or*

(d) $n = p^\alpha q^\beta$ *and* p *or* $q \equiv 3 \pmod 4$*;*

(3) $\operatorname{ord}_n\big((\frac{n-1}{2})_n!\big) = 1$ *in all other cases.*

We actually show more in this paper: In all cases the value of $\big(\frac{n-1}{2}\big)_n! \pmod n$ is either given explicitly or is easily computable, and in several cases there are partial results concerning $\big(\frac{n-1}{M}\big)_n!$ for integers $M \geq 2$ and certain classes of integers $n \equiv 1 \pmod M$. These results can be found in Sections 3–5.

For the proof of Theorem 2 we will have to distinguish between the cases where the modulus n has one, two, or at least three distinct prime divisors. These cases will be dealt with in Sections 2, 4, and 5, respectively, while the most central arguments will be given in Section 3. In Section 6 we deal, without proofs, with $\big\lfloor\frac{n-1}{2}\big\rfloor_n!$ for even n, and we conclude this paper with some additional remarks in Section 7.

2. One Prime Divisor

We begin with a general discussion of the Gauss factorial $\big(\frac{n-1}{2}\big)_n!$ for odd integers $n \geq 3$. Since $(n-1)_n!$ has $\varphi(n)$ factors, we obtain by the same symmetry argument as in (4),

$$\big(\tfrac{n-1}{2}\big)_n!^2 \equiv (-1)^{\frac{1}{2}\varphi(n)+\varepsilon} \pmod n, \tag{10}$$

where, by (3), $\varepsilon = 1$ when $n = p^\alpha$, and $\varepsilon = 0$ otherwise. Now $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$, and therefore

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

On the other hand, $\varphi(n)$ is divisible by 4 if n has at least two distinct odd prime factors. Hence with (10) we get

$$\big(\tfrac{n-1}{2}\big)_n!^2 \equiv \begin{cases} -1 \pmod n & \text{if } \ n = p^\alpha,\ p \equiv 1 \pmod 4, \\ 1 \pmod n & \text{otherwise.} \end{cases} \tag{11}$$

This immediately gives the partial result

$$\operatorname{ord}_n\left(\left(\tfrac{n-1}{2}\right)_n!\right) = 4 \quad \text{for} \quad n = p^\alpha,\ p \equiv 1 \pmod 4, \tag{12}$$

which extends (6).

In order to deal with the case $p \equiv 3 \pmod 4$, we first prove an easy lemma, which will also be used later.

Lemma 1. *Let p be an odd prime and $\alpha \geq 1$ an integer. If the integer A is such that $A^2 \equiv 1 \pmod{p^\alpha}$, then $A \equiv \pm 1 \pmod p$ if and only if $A \equiv \pm 1 \pmod{p^\alpha}$, with the signs corresponding to each other.*

Proof. One direction is obvious. For the other direction, write $A = kp \pm 1$. Then $A^2 = k^2p^2 \pm 2kp + 1$, and thus we require $p^\alpha \mid k^2p^2 \pm 2kp$, i.e., $p^{\alpha-1} \mid k(kp \pm 2)$. Since p is odd, this means that $p^{\alpha-1} \mid k$, and therefore $A = \ell p^{\alpha-1}p \pm 1$ for some integer ℓ. This completes the proof. □

By (11), this lemma means that it suffices to determine $\left(\frac{n-1}{2}\right)_n! \pmod p$ when $n = p^\alpha, p \equiv 3 \pmod 4$. To do this, we first observe that

$$\frac{p^\alpha - 1}{2} = \frac{p^{\alpha-1} - 1}{2}p + \frac{p-1}{2},$$

in other words, $\frac{p^\alpha-1}{2}$ leaves remainder $\frac{p-1}{2}$ when divided by p. If we denote $r = (p^{\alpha-1} - 1)/2$, then we can write

$$\begin{aligned}\left(\tfrac{p^\alpha-1}{2}\right)_{p^\alpha}! &= \big(1 \cdot 2 \cdot \ldots \cdot (p-1)\big)\big((p+1) \cdot \ldots \cdot (2p-1)\big) \cdot \ldots \\ &\quad \cdot \big((rp - p + 1) \cdot \ldots \cdot (rp-1)\big) \cdot \big((rp+1) \cdot \ldots \cdot (rp + \tfrac{p-1}{2})\big) \\ &\equiv (p-1)!^r \left(\tfrac{p-1}{2}\right)! \pmod p.\end{aligned}$$

Since $p \equiv -1 \pmod 4$, r is even if and only if $\alpha - 1$ is even, and by Wilson's theorem (1) we therefore have

$$\left(\tfrac{p^\alpha-1}{2}\right)_{p^\alpha}! \equiv (-1)^{\alpha-1}\left(\tfrac{p-1}{2}\right)! \pmod p. \tag{13}$$

With (8) and Lemma 1 we have therefore obtained the following partial result.

Proposition 1. *For $p \equiv 3 \pmod 4$,*

$$\left(\tfrac{p^\alpha-1}{2}\right)_{p^\alpha}! \equiv \begin{cases} (-1)^\alpha \pmod{p^\alpha} & \text{if} \quad p > 3 \text{ and } h(-p) \equiv 1 \pmod 4, \\ (-1)^{\alpha-1} \pmod{p^\alpha} & \text{otherwise.} \end{cases} \tag{14}$$

As an illustration of this, see the powers of 3, 7 and 11 in Table 1.

3. An Auxiliary Result

While the case of one prime divisor holds in the above form only for $\left(\frac{n-1}{2}\right)_n!$, in the remaining cases we can obtain more general partial results for $\left(\frac{n-1}{M}\right)_n!$, $M \geq 2$, with only moderate additional effort. The following result will be instrumental for the next two sections.

Proposition 2. *Let $M \geq 2$ and $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ with $t \geq 2$ and $\alpha_j \geq 1$ for $j = 1, 2, \dots, t$. Suppose that $n \equiv p_t \equiv 1 \pmod{M}$ and $p_j \equiv 1 \pmod{M}$ for at least one other index $j, 1 \leq j \leq t-1$. Then*

$$\left(\tfrac{n-1}{M}\right)_n! \equiv \frac{\varepsilon^{(p_t-1)/M}}{p_t^A} \pmod{p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}}}, \tag{15}$$

where $\varepsilon = -1$ when $t = 2$, $\varepsilon = 1$ when $t \geq 3$, and

$$A = \frac{1}{M} p_t^{\alpha_t - 1} \varphi(p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}}).$$

Proof. To simplify notation, we set

$$\widetilde{n} = p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}}, \qquad s = \frac{p_t^{\alpha_t} - 1}{M}. \tag{16}$$

The idea now is to apply the Gauss-Wilson theorem for $\widetilde{n}$ to the left-hand side of (15). For this purpose we divide $\frac{n-1}{M}$ by $\widetilde{n}$ with remainder:

$$\frac{n-1}{M} = s\widetilde{n} + \frac{\widetilde{n}-1}{M}, \tag{17}$$

which is obvious from (16). Note that by hypothesis we know that s and $(\widetilde{n}-1)/M$ are both integers. Based on (17) we split the Gauss factorial in (15) into s products of similar lengths and into one shorter product, i.e., we write

$$\left(\tfrac{n-1}{M}\right)_n! = \left(\prod_{j=1}^{s} P_j\right) Q, \tag{18}$$

where

$$P_j = \prod_{\substack{k=1 \\ \gcd(k,n)=1}}^{\widetilde{n}-1} \big((j-1)\widetilde{n} + k\big), \qquad Q = \prod_{\substack{k=1 \\ \gcd(k,n)=1}}^{\frac{\widetilde{n}-1}{M}} \big(s\widetilde{n} + k\big). \tag{19}$$

Now, if in each product P_j the indices k were relatively prime to just $\widetilde{n}$, then by the Gauss-Wilson theorem (3) they would all be congruent to $-1 \pmod{\widetilde{n}}$ if $t = 2$, or $1 \pmod{\widetilde{n}}$ if $t \geq 3$. To deal with this, we multiply all relevant multiples of p_t back into $P_1, \dots, P_s$, and Q. More exactly, on the right-hand side of (18) we multiply numerator and denominator by

$$\prod \{(jp_t) \mid 1 \leq j \leq s', \gcd(j, \widetilde{n}) = 1\}, \tag{20}$$

i.e., by the product of the elements in the set, where

$$s' = \frac{1}{M}\left(p_1^{\alpha_1} \cdot \ldots \cdot p_{t-1}^{\alpha_{t-1}} p_t^{\alpha_t - 1} - 1\right),$$

which comes from the obvious division

$$\frac{n-1}{M} = s' p_t + \frac{p_t - 1}{M}, \tag{21}$$

where s' and $(p_t - 1)/M$ are integers, by hypothesis. To count the number of elements in the set in (20), we do yet another obvious division with remainder, namely

$$s' = \frac{1}{M}\left(p_t^{\alpha_t - 1} - 1\right)\widetilde{n} + \frac{\widetilde{n} - 1}{M}. \tag{22}$$

The contributions to (20) from each of the intervals of length $\widetilde{n}$ are no problem; they are just $\varphi(\widetilde{n})$. However, in order to deal with the remainder term in (22) we need the following lemma.

Lemma 2. *Let $M \geq 2$ and $n = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ with $n \equiv p_t \equiv 1 \pmod{M}$. Then*

$$\#\{j \mid 1 \leq j \leq \tfrac{n-1}{M}, \gcd(j, n) = 1\} = \frac{1}{M}\varphi(n). \tag{23}$$

Proof. Lehmer [12, Theorem 4] showed that when n has a prime divisor $p \equiv 1 \pmod{M}$, the *totatives* of n are uniformly distributed, i.e., the intervals

$$(k-1)\frac{n}{M} < j < k\frac{n}{M}, \qquad k = 1, 2, \ldots, M,$$

have equal numbers of integers j relatively prime to n, and the endpoints cannot themselves be totatives. Hence the number of totatives in the interval $0 < j < n/M$, and thus also for $1 \leq j \leq (n-1)/M$, is $\varphi(n)/M$. This completes the proof. □

Returning to the proof of (15), we use (22) and (23) with $\widetilde{n}$ in place of n, and see that the cardinality of the set in (20) is

$$\frac{1}{M}\left(p_t^{\alpha_t - 1} - 1\right)\varphi(\widetilde{n}) + \frac{1}{M}\varphi(\widetilde{n}) = \frac{1}{M} p_t^{\alpha_t - 1}\varphi(\widetilde{n}). \tag{24}$$

If we denote this number by A, we get from (18),

$$\left(\tfrac{n-1}{M}\right)_n! \equiv \frac{\overline{P_1} \cdot \ldots \cdot \overline{P_s} \cdot \overline{Q}}{p_t^A \prod\{j \mid 1 \leq j \leq s', \gcd(j, \widetilde{n}) = 1\}} \pmod{\widetilde{n}}. \tag{25}$$

Here the bars over the P_j and Q indicate that the products (19) are taken over all k relatively prime to $\widetilde{n}$ (instead of n). But then the Gauss-Wilson theorem gives

$$\overline{P_1} \equiv \ldots \equiv \overline{P_s} \equiv \begin{cases} -1 \pmod{\widetilde{n}} & \text{if } t = 2, \\ 1 \pmod{\widetilde{n}} & \text{if } t \geq 3. \end{cases} \tag{26}$$

From the second part of (19) we get

$$\overline{Q} \equiv \prod_{\substack{k=1 \\ \gcd(k,\widetilde{n})=1}}^{\frac{\widetilde{n}-1}{M}} k. \tag{27}$$

The product in the denominator of (25) can be split up into $(p_t^{\alpha_t-1}-1)/M$ products that are congruent to the $\overline{P_j}$ and a remainder that is congruent to $\overline{Q} \pmod{\widetilde{n}}$; this follows from (22). Hence (26) and (27) together with (25) give

$$\left(\tfrac{n-1}{M}\right)_n! \equiv \frac{\varepsilon^B}{p_t^A} \pmod{\widetilde{n}}, \tag{28}$$

with A defined by (24) and

$$B = s - \frac{p_t^{\alpha_t-1}-1}{M} = p_t^{\alpha_t-1}\frac{p_t-1}{M}.$$

Since p_t is odd, this completes the proof of the proposition. □

4. Two Prime Divisors

When $n = p^\alpha q^\beta$ with p and q odd primes and $\alpha, \beta \geq 1$, then by (11) we have

$$\left(\tfrac{n-1}{2}\right)_n!^2 \equiv 1 \pmod{n}.$$

This may or may not mean that $\left(\frac{n-1}{2}\right)_n! \equiv \pm 1 \pmod{n}$. The following result provides a classification of the situation. Here $\left(\frac{p}{q}\right)$ is the Legendre symbol, as usual.

Proposition 3. *Let n be as above. Then*

$$\left(\tfrac{n-1}{2}\right)_n! \equiv \left(\frac{p}{q}\right) \pmod{n} \quad \textit{if} \quad p \equiv q \equiv 1 \pmod{4}, \tag{29}$$

while

$$\left(\tfrac{n-1}{2}\right)_n! \not\equiv \pm 1 \pmod{n} \quad \textit{if} \quad p \textit{ or } q \equiv 3 \pmod{4}. \tag{30}$$

For the proof of this result we require the following lemma which is a direct consequence of Proposition 2.

Lemma 3. *With n as above, we have*

$$\left(\tfrac{n-1}{2}\right)_n! \equiv \frac{(-1)^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} \pmod{p^\alpha}. \tag{31}$$

Proof. We use Proposition 2 with $M = 2, t = 2, p_1 = p, p_2 = q, \alpha_1 = \alpha$, and $\alpha_2 = \beta$. Then the hypotheses are satisfied, and also

$$A = \frac{1}{2}q^{\beta-1}\varphi(p^\alpha) = \frac{p-1}{2}p^{\alpha-1}q^{\beta-1},$$

and since $q^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, while the powers of p and q are odd, we obtain from (15),

$$\left(\tfrac{n-1}{2}\right)_n! \equiv \frac{(-1)^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} \pmod{p}.$$

Lemma 1 now immediately gives (31). □

Proof of Proposition 3. By symmetry, (31) is equivalent to

$$\left(\tfrac{n-1}{2}\right)_n! \equiv \frac{(-1)^{\frac{p-1}{2}}}{p^{\frac{q-1}{2}}} \pmod{q^\beta}. \tag{32}$$

If $p \equiv q \equiv 1 \pmod 4$, then the numerators in (31) and (32) are both 1, while by Euler's criterion we have

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

and by quadratic reciprocity the two Legendre symbols are the same. Hence $\left(\frac{n-1}{2}\right)_n! \equiv \left(\frac{p}{q}\right)$ (mod p) and (mod q), and by Lemma 1 this can be lifted to the moduli p^α and q^β. The congruence (29) now follows from the Chinese Remainder Theorem.

On the other hand, if at least one of p and q is $\equiv 3 \pmod 4$ then either the numerators of (31) and (32) are the same and the denominators differ, by quadratic reciprocity (if $p \equiv q \equiv 3 \pmod 4$), or the numerators differ and the denominators are the same (if p and q are in different residue classes (mod 4)). Hence, again after using Lemma 1, we see that modulo $n = p^\alpha q^\beta$ the Gauss factorial $\left(\frac{n-1}{2}\right)_n!$ can be neither 1 nor -1. This completes the proof of the proposition. □

Numerous examples for Proposition 3 can be found in Table 1.

5. Three or More Prime Divisors

We continue with the case where n has at least three distinct prime divisors. With a little additional effort we can obtain the following more general result.

Proposition 4. *Let $M \geq 2$ and $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, $t \geq 3$, with arbitrary positive exponents α_j. If $n \equiv 1 \pmod M$ and $p_j \equiv 1 \pmod M$ for at least three indices from among $1, 2, \dots, t$, then*

$$\left(\tfrac{n-1}{M}\right)_n! \equiv 1 \pmod{n}. \tag{33}$$

Proof. Without loss of generality we may assume that $p_{t-1} \equiv p_t \equiv 1 \pmod{M}$, and we claim that

$$\left(\tfrac{n-1}{M}\right)_n! \equiv 1 \pmod{p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}}}. \tag{34}$$

Then by symmetry we have

$$\left(\tfrac{n-1}{M}\right)_n! \equiv 1 \pmod{p_1^{\alpha_1} \dots p_{t-2}^{\alpha_{t-2}} p_t^{\alpha_t}},$$

and the Chinese Remainder Theorem applied to these two congruences immediately gives (33).

In order to prove (34) we use Proposition 2 again and note that the numerator of (15) is 1 since $t \geq 3$. To evaluate the denominator, we need the following lemma.

Lemma 4. *Let $m \geq 2$ and $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, $t \geq 2$. If at least two of the primes $p_1, \dots, p_t$ satisfy $p_j \equiv 1 \pmod{M}$, then for any integer a coprime to n we have*

$$a^{\varphi(n)/M} \equiv 1 \pmod{n}. \tag{35}$$

Proof. By reordering, if necessary, we may assume that $p_1 \equiv p_2 \equiv 1 \pmod{M}$. Now for $j = 1, 2$ we have

$$\frac{\varphi(n)}{M} = \frac{p_j - 1}{M} p_j^{\alpha_j - 1} \varphi(n/p_j^{\alpha_j}),$$

where $k_j = \frac{p_j - 1}{M} p_j^{\alpha_j - 1}$ is an integer. Hence Euler's generalization of Fermat's Little Theorem gives

$$a^{\varphi(n)/M} = \left(a^{\varphi(n/p_j^{\alpha_j})}\right)^{k_j} \equiv 1 \pmod{n/p_j^{\alpha_j}},$$

and with the Chinese Remainder Theorem we get (35). □

Using this lemma with $\widetilde{n}$ for n and p_t for a, we immediately obtain $p_t^A \equiv 1 \pmod{\widetilde{n}}$, which with (35) and (15) proves (34); this completes the proof of the proposition. □

Proposition 4 is best possible in the sense that (33) usually does not hold when only two of the primes $p_1, \dots, p_t$ satisfy $p_j \equiv 1 \pmod{M}$. This is illustrated by the following (smallest possible) example:

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

$$\left(\tfrac{n-1}{3}\right)_n! = 121_{364}! \equiv 113 \pmod{364}.$$

Also, the multiplicative order of $113 \pmod{364}$ is 3. This example points to more general results which, however, would go beyond the scope of this paper.

As an immediate consequence of Proposition 4 we obtain the following result, which concludes the proof of Theorem 2.

Corollary 2. *For all odd n with at least three distinct prime divisors we have*

$$\left(\tfrac{n-1}{2}\right)_n! \equiv 1 \pmod{n}. \tag{36}$$

Table 1 may serve as an illustration of this.

6. Even Moduli n

Obviously $(\frac{n-1}{2})_n!$ makes sense only for odd n. However, it turns out that we do get meaningful results if we use the greatest integer not exceeding $(n-1)/2$, i.e., if we consider

$$\left\lfloor\tfrac{n-1}{2}\right\rfloor_n! \pmod{n}.$$

The same methods as in the previous sections can be used to deal with this case, and the results are very similar. We therefore skip the proofs.

n	factored	$b(n)$	$b(n)^2$	n	factored	$b(n)$	$b(n)^2$
202	$2 \cdot 101$	-91	-1	252	$2^2 \cdot 3^2 \cdot 7$	1	1
204	$2^2 \cdot 3 \cdot 17$	1	1	254	$2 \cdot 127$	1	1
206	$2 \cdot 103$	1	1	256	2^8	-127	1
208	$2^4 \cdot 13$	1	1	258	$2 \cdot 3 \cdot 43$	-85	1
210	$2 \cdot 3 \cdot 5 \cdot 7$	1	1	260	$2^2 \cdot 5 \cdot 13$	1	1
212	$2^2 \cdot 53$	105	1	262	$2 \cdot 131$	-1	1
214	$2 \cdot 107$	1	1	264	$2^3 \cdot 3 \cdot 11$	1	1
216	$2^3 \cdot 3^3$	1	1	266	$2 \cdot 7 \cdot 19$	113	1
218	$2 \cdot 109$	-33	-1	268	$2^2 \cdot 67$	133	1
220	$2^2 \cdot 5 \cdot 11$	1	1	270	$2 \cdot 3^3 \cdot 5$	-109	1
222	$2 \cdot 3 \cdot 37$	73	1	272	$2^4 \cdot 17$	1	1
224	$2^5 \cdot 7$	1	1	274	$2 \cdot 137$	37	-1
226	$2 \cdot 113$	15	-1	276	$2^2 \cdot 3 \cdot 23$	1	1
228	$2^2 \cdot 3 \cdot 19$	1	1	278	$2 \cdot 139$	1	1
230	$2 \cdot 5 \cdot 23$	91	1	280	$2^3 \cdot 5 \cdot 7$	1	1
232	$2^3 \cdot 29$	1	1	282	$2 \cdot 3 \cdot 47$	-95	1
234	$2 \cdot 3^2 \cdot 13$	-53	1	284	$2^2 \cdot 71$	141	1
236	$2^2 \cdot 59$	117	1	286	$2 \cdot 11 \cdot 13$	131	1
238	$2 \cdot 7 \cdot 17$	69	1	288	$2^5 \cdot 3^2$	1	1
240	$2^4 \cdot 3 \cdot 5$	1	1	290	$2 \cdot 5 \cdot 29$	1	1
242	$2 \cdot 11^2$	1	1	292	$2^2 \cdot 73$	145	1
244	$2^2 \cdot 61$	121	1	294	$2 \cdot 3 \cdot 7^2$	-97	1
246	$2 \cdot 3 \cdot 41$	83	1	296	$2^3 \cdot 37$	1	1
248	$2^3 \cdot 31$	1	1	298	$2 \cdot 149$	105	-1
250	$2 \cdot 5^3$	-57	-1	300	$2^2 \cdot 3 \cdot 5^2$	1	1

Table 2: $b(n) \equiv \left\lfloor\frac{n-1}{2}\right\rfloor_n! \pmod{n}$ for even n, $202 \le n \le 300$.

We begin by stating the explicit values for $\left\lfloor \frac{n-1}{2} \right\rfloor_n!$ or its square (modulo n) in various cases, before summarizing the orders in a way similar to Theorem 2. To illustrate the results below we list 50 consecutive even cases of n in Table 2.

Case 1. $n = 2^r, r \geq 3$. Then

$$\left\lfloor \tfrac{n-1}{2} \right\rfloor_n! \equiv 1 - \tfrac{n}{2} \pmod{n}.$$

Case 2. $n = 2^r p^\alpha$, p an odd prime, and $r, \alpha \geq 1$. Then

$$\left\lfloor \tfrac{n-1}{2} \right\rfloor_n! \equiv \begin{cases} \frac{n}{2} - 1 \pmod{n} & \text{for} \quad r = 2, \\ 1 \pmod{n} & \text{for} \quad r \geq 3. \end{cases}$$

Furthermore, when $r = 1$ and $p \equiv 1 \pmod 4$, we have

$$\left\lfloor \tfrac{n-1}{2} \right\rfloor_n!^2 \equiv -1 \pmod{n},$$

and when $r = 1$ and $p \equiv 3 \pmod 4$,

$$\left\lfloor \tfrac{n-1}{2} \right\rfloor_n! \equiv (-1)^\alpha \left(\tfrac{2}{p}\right) (-1)^{\frac{h(-p)+1}{2}} \pmod{n},$$

where $(\frac{2}{p})$ is the Legendre symbol and, as before, $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$. Compare the right-hand side of the last congruence with (37) below. Also, recall the well-known evaluation $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

Case 3. $n = 2^r p^\alpha q^\beta$, $p \neq q$ odd primes, and $r, \alpha, \beta \geq 1$. Then for $p \equiv q \equiv 1 \pmod 4$,

$$\left\lfloor \tfrac{n-1}{2} \right\rfloor_n! \equiv \begin{cases} -1 \pmod{n} & \text{if} \quad r = 1 \quad \text{and} \quad (\frac{p}{q}) = -1, \\ 1 \pmod{n} & \text{otherwise,} \end{cases}$$

and if $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$ then for $r = 1$,

$$\left\lfloor \tfrac{n-1}{2} \right\rfloor_n!^2 \equiv 1 \pmod{n} \quad \text{but} \quad \left\lfloor \tfrac{n-1}{2} \right\rfloor_n! \not\equiv \pm 1 \pmod{n},$$

while for $r \geq 2$,

$$\left\lfloor \tfrac{n-1}{2} \right\rfloor_n! \equiv 1 \pmod{n}.$$

Case 4. n has at least three distinct odd prime factors. Then

$$\left\lfloor \tfrac{n-1}{2} \right\rfloor_n! \equiv 1 \pmod{n}.$$

We now summarize the above cases by giving the multiplicative orders modulo n; compare this with Theorem 2.

Theorem 3. *Let $n \geq 4$ be an even integer, p and q distinct odd primes, and let r, α, and β be positive integers. Then*

(1) $\operatorname{ord}_n\left(\left\lfloor \frac{n-1}{2} \right\rfloor_n !\right) = 4$ *when* $n = 2p^\alpha$ *and* $p \equiv 1 \pmod 4$;

(2) $\operatorname{ord}_n\left(\left\lfloor \frac{n-1}{2} \right\rfloor_n !\right) = 2$ *when*

(a) $n = 2^r$, $r \geq 3$, *or*

(b) $n = 4p^\alpha$, *or*

(c) $n = 2p^\alpha$, $p \equiv 3 \pmod 4$, $p > 3$, *and* $\frac{p^2-1}{8} + \frac{h(-p)+1}{2} \not\equiv \alpha \pmod 2$, *or*

(d) $n = 2 \cdot 3^\alpha$, $\alpha \equiv 0 \pmod 2$, *or*

(e) $n = 2p^\alpha q^\beta$, $p \equiv q \equiv 1 \pmod 4$, *and* $\left(\frac{p}{q}\right) = -1$, *or*

(f) $n = 2p^\alpha q^\beta$ *and* p *or* $q \equiv 3 \pmod 4$;

(3) $\operatorname{ord}_n\left(\left\lfloor \frac{n-1}{2} \right\rfloor_n !\right) = 1$ *in all other cases.*

We illustrate this result by considering all the cases of $n = 2p^\alpha$ listed in Table 2. For $n = 202, 218, 226, 250, 274$, and 298 we have $p \equiv 1 \pmod 4$, and thus by (1) the order is 4.

In the case $p \equiv 3 \pmod 4$, part (2)(c) of Theorem 3 has to be invoked; we list the n in question in Table 3 below.

n	$\frac{p^2-1}{8} \pmod 2$	$\frac{h(-p)+1}{2}$	α	$\operatorname{ord}_n\left(\left\lfloor \frac{n-1}{2} \right\rfloor_n !\right)$
$2 \cdot 103$	0	3	1	1
$2 \cdot 107$	1	2	1	1
$2 \cdot 11^2$	1	1	2	1
$2 \cdot 127$	0	3	1	1
$2 \cdot 131$	1	3	1	2
$2 \cdot 139$	1	2	1	1

Table 3: $n = 2p^\alpha$, $p \equiv 3 \pmod 4$, $202 \leq n \leq 300$.

The values of the class number $h(-p)$ can be found, e.g., in [2, p. 425], or can be computed with the number theoretic computer algebra system PARI/GP [15]. We see in Table 3 that the relation in (2)(c) holds only for $n = 2 \cdot 131$, which is consistent with the order being 2 in this case, while it is 1 in the remaining five cases.

7. Further Remarks

1. In spite of the fact that the Gauss-Wilson theorem was stated in the famous *Disqusitiones Arithmeticae* [7, §78] and in the equally influential books [6, §38] and [9, p. 102], surprisingly little can be found on this topic in the literature. The few published references to this result include [10] and [17], where Theorem 1 was further extended, and [11] and [1], where (3) was used to extend the classical *Wilson quotient* to composite moduli. The theorem was rediscovered at least once; see [16].

2. While some partial results are known for the values or the orders (modulo n) of $\left(\frac{n-1}{M}\right)_n!$ for arbitrary integers $M \geq 2$, the case $M = 2$, treated in this paper, is the only one that is completely characterized. In fact, in no other case is the order bounded. Partial results on the cases $M = 3$ and $M = 4$ will be the subject of forthcoming work by the authors.

3. It would not have been possible to find the results in this paper without the use of computer algebra. In fact, extensive use was made of the computer algebra system Maple, versions 7 – 9 (the current version at the time of writing is Maple 11; see [13]).

4. Mordell [14] remarks in his paper that the result (9) was independently discovered by Chowla. A proof is also given in [18, Theorem 8]. Professor A. Schinzel kindly informed us that this result can also be found in a book by Venkov, both in the English translation [19, p. 9] of 1970 and already in the Russian original published in 1937. This is the earliest mention we could find of this result, and Venkov may have been the first to prove it; no reference is given.

A different criterion for the sign in (8) is due to Kronecker and can be found in Venkov's book [19, p. 227]. For a brief account of the earlier history of this problem, see [5, p. 275–276].

5. The relation (9) can be written more concisely as

$$\left(\tfrac{p-1}{2}\right)! \equiv (-1)^{\frac{h(-p)+1}{2}} \pmod{p}, \tag{37}$$

where $p \equiv 3 \pmod 4$, $p > 3$, is a prime. This result of Venkov and Mordell was extended by Chowla [4] (see also [18, Theorem 9]) to primes $p \equiv 1 \pmod 4$ as follows. Let $\varepsilon_p = (u_p + v_p\sqrt{p})/2 > 1$ be the fundamental unit and $h(p)$ the class number of the *real* quadratic field $\mathbb{Q}(\sqrt{p})$. Then

$$\left(\tfrac{p-1}{2}\right)! \equiv \tfrac{1}{2}(-1)^{\frac{h(p)+1}{2}} u_p \pmod{p}. \tag{38}$$

Since ε_p is a unit, we have $u_p^2 + pv_p^2 = \pm 4$, and it follows from (38) that $\left(\frac{p-1}{2}\right)!^4 \equiv 1 \pmod p$, which is consistent with (7). On the other hand, (7) shows that we have $u_p^2 + pv_p^2 = -4$, i.e., the norm of ε_p is -1; this was also observed in [3].

6. Recently Chapman and Pan [3] found q-analogues of the congruences (37) and (38), as well as of Wilson's congruence (1).

References

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

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[3] R. Chapman and H. Pan, *q-analogues of Wilson's theorem*, Int. J. Number Theory **4** (2008), 539–547.

[4] S. Chowla, *On the class number of real quadratic fields*, Proc. Nat. Acad. Sci. USA **47** (1961), 878.

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

[6] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, edited and supplemented by R. Dedekind, 4th edition, Chelsea Publishing Company, New York, 1968. English translation: *Lectures on Number Theory*, translated by J. Stillwell, American Mathematical Society, Providence, 1999.

[7] C. F. Gauss, *Disquisitiones Arithmeticae*. Translated and with a preface by Arthur A. Clarke. Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse. Springer-Verlag, New York, 1986. xx+472 pp.

[8] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*. Organic mathematics (Burnaby, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997.

[9] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Oxford University Press, 1979.

[10] P. Kesava Menon, *A generalization of Wilson's theorem*, J. Indian Math. Soc. (N.S.) **9** (1945), 79–88.

[11] K. E. Kloss, *Some number theoretic calculations*, J. Res. Nat. Bureau of Stand., B, **69** (1965), 335–339.

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

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

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

[15] PARI/GP, `http://pari.math.u-bordeaux.fr/`.

[16] S. Sanielevici, *Une généralisation du théorme de Wilson*, Com. Acad. R. P. Romîne **8** (1958), 737–744.

[17] Š. Schwarz, *The role of semigroups in the elementary theory of numbers*, Math. Slovaca **31** (1981), 369–395.

[18] J. Urbanowicz and K. S. Williams, *Congruences for L-functions*, Kluwer Academic Publishers, Dordrecht, 2000.

[19] B. A. Venkov, *Elementary Number Theory*, Wolters-Noordhoff Publishing, Groningen, 1970.