



The Congruence $(p - 1/2)! \equiv \pm 1 \pmod{p}$

Author(s): L. J. Mordell

Source: *The American Mathematical Monthly*, Vol. 68, No. 2 (Feb., 1961), pp. 145-146

Published by: Mathematical Association of America

Stable URL: <http://www.jstor.org/stable/2312481>

Accessed: 20/06/2009 18:29

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=maa>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit organization founded in 1995 to build trusted digital archives for scholarship. We work with the scholarly community to preserve their work and the materials they rely upon, and to build a common research platform that promotes the discovery and use of these resources. For more information about JSTOR, please contact support@jstor.org.



Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

<http://www.jstor.org>

References

1. J. W. L. Glaisher, Formulae for partitions into given elements, derived from Sylvester's theorem, *Quart. J. Math.*, vol. 40, 1909, pp. 275-348.
2. G. J. Rieger, Über Partitionen, *Math. Ann.*, vol. 138, 1959, pp. 356-362.
3. J. J. Sylvester, Excursus on rational fractions and partitions, *Amer. J. Math.*, vol. 5, 1882, pp. 119-136.

THE CONGRUENCE $(p-1/2)! \equiv \pm 1 \pmod{p}$

L. J. MORDELL, University of Colorado and St. John's College, Cambridge, England

Let p be an odd prime. Then Wilson's classical result states that $(p-1)! + 1 \equiv 0 \pmod{p}$. On noting that $p-r \equiv -r \pmod{p}$, this gives, when $p \equiv 1 \pmod{4}$, as is well known,

$$\left\{ \left(\frac{p-1}{2} \right)! \right\}^2 + 1 \equiv 0 \pmod{p}.$$

However, when $p \equiv 3 \pmod{4}$, we have

$$\left\{ \left(\frac{p-1}{2} \right)! \right\}^2 - 1 \equiv 0 \pmod{p}.$$

Hence

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

where $a = 0$ or 1 . In view of the history of the question, it may perhaps be worth while to state and prove the

THEOREM.* *If p is a prime $\equiv 3 \pmod{4}$ and $p > 3$, then in (1)*

$$(2) \quad a \equiv \frac{1}{2}[1 + h(-p)] \pmod{2}$$

where $h(-p)$ is the class number of the quadratic field $k\{\sqrt{-p}\}$.

This result does not appear to have been explicitly stated or at any rate does not seem well known. It is, however, implicit in the literature, and it is now a trivial deduction from results long known, e.g., an old one of Dirichlet's (1828) given here as (3). In fact, Jacobi (1832) conjectured a result equivalent to (2) at a time when the class-number formula was not known. For the history of the subject, see Dickson's *History of the Theory of Numbers*, Vol. 1, page 275.

Write $E = [\frac{1}{2}(p-1)]!$. Denote by r_1, r_2, \dots the R quadratic residues of p less than $\frac{1}{2}p$, and by n_1, n_2, \dots the N quadratic nonresidues less than $\frac{1}{2}p$. Then the quadratic residues r'_1, r'_2, \dots greater than $\frac{1}{2}p$ are given by $p-n_1, p-n_2, \dots$ since $p \equiv 3 \pmod{4}$. Then

$$(3) \quad E = r_1 r_2 \dots n_1 n_2 \dots \equiv (-1)^N r_1 r_2 \dots r'_1 r'_2 \dots \equiv (-1)^N \pmod{p} \text{ if } p > 3,$$

* Professor Chowla informs me that he found the result about the same time that I did.

since $(-1)^NE \equiv g^{2+4+\dots+(p-1)} = g^{\frac{1}{2}(p^2-1)} = (g^{\frac{1}{2}(p+1)})^{\frac{1}{2}(p+1)} \equiv 1 \pmod{p}$, where g is a primitive root of p .

Now $R+N = \frac{1}{2}(p-1)$, and it is known* from the class-number formula that

$$R - N = \delta h(-p), \quad \begin{cases} \delta = 1 & \text{if } p \equiv 7 \pmod{8}, \\ \delta = 3 & \text{if } p \equiv 3 \pmod{8}, p > 3. \end{cases}$$

Hence $2N = \frac{1}{2}(p-1) - \delta h(-p)$. Then if $p \equiv 7 \pmod{8}$, $2N \equiv 3 - h(-p) \pmod{4}$, and if $p \equiv 3 \pmod{8}$, $2N \equiv 1 - 3h(-p) \pmod{4}$. The first is $N \equiv \frac{1}{2}[-1 - h(-p)] \pmod{2}$ and the second is $N \equiv \frac{1}{2}[1 + h(-p)] \pmod{2}$. These are both included in $N \equiv \frac{1}{2}[1 + h(-p)] \pmod{2}$.

* L. Holzer, *Zahlentheorie II*, 1959, Leipzig, pp. 91-93, and H. Hasse, *Vorlesungen über Zahlentheorie*, 1950, Berlin, pp. 386-390.

A GENERALIZED TURÁN EXPRESSION FOR THE BESSEL FUNCTIONS

WALFED A. AL-SALAM, University of Baghdad, Iraq

1. In a recent paper Toscano [3] has proved the formula

$$(1.1) \quad \sum_{r=-m}^m (-1)^r \binom{2m}{m-r} H_{n+r}(x) H_{n-r}(x) = \frac{(2m)!(n-m)!}{m!} \sum_{j=m}^n \binom{j-1}{m-1} \frac{H_{n-j}^2(x)}{(n-j)!} \quad (m \leq n)$$

where $H_n(x)$ is the Hermite polynomial of order n . The expression in the left hand side may be regarded as a generalization of the Turán expression $H_n^2(x) - H_{n+1}(x)H_{n-1}(x)$. Indeed (1.1) reduces to the Demir-Hsü formula [2] when $m=1$. Other proofs of (1.1) as well as extensions to the Laguerre and ultraspherical polynomials and other hypergeometric functions are given in [1].

In the present note we obtain a similar formula involving the Bessel functions. We prove

$$(1.2) \quad \begin{aligned} \Omega_n^{(m)}(x) &= \sum_{r=-m}^m (-1)^r \binom{2m}{m-r} J_{n-r}(x) J_{n+r}(x) \\ &= \frac{4^m (2m)!}{x^{2m} m! (m-1)!} \sum_{k=0}^{\infty} (n+m+2k)(k+1)_{m-1} (n+k-1)_{m-1} J_{n+m+2k}^2(x) \end{aligned}$$

where $(a)_m = a(a+1)(a+2) \dots (a+m-1)$, $(a)_0 = 1$. For definition of the Bessel function $J_n(x)$ see [4]. This formula reduces, for $m=1$, to Lommel's formula [4, p. 152]

$$(1.3) \quad \frac{1}{4} x^2 \{ J_n^2(x) - J_{n+1}(x) J_{n-1}(x) \} = \frac{1}{4} x^2 \Delta_n(x) = \sum_{k=0}^{\infty} (n+1+2k) J_{n+1+2k}^2(x).$$

It is also a positive representation as sum of squares.