Extending Babbage’s (Non-)Primality Tests

Jonathan Sondow

Abstract We recall Charles Babbage’s 1819 criterion for primality, based on simultaneous congruences for binomial coefficients, and extend it to a least-prime-factor test. We also prove a partial converse of his non-primality test, based on a single congruence. Two problems are posed. Along the way we encounter Bachet, Bernoulli, Bézout, Euler, Fermat, Kummer, Lagrange, Lucas, Vandermonde, Waring, Wilson, Wolstenholme, and several contemporary mathematicians.

1 Introduction

Charles Babbage was an English mathematician, philosopher, inventor, mechanical engineer, and “irascible genius” who pioneered computing machines [2, 4, 10, 21, 22, 23]. Although he held the Lucasian Chair of Mathematics at Cambridge University from 1828 to 1839, during that period he never resided in Cambridge or delivered a lecture [5, 7, p. 7].

Charles Babbage (1791–1871)

In 1819 he published his only work on number theory, a short paper [1] that begins:

209 West 97th Street, New York, NY 10025 jsondow@alumni.princeton.edu
The singular theorem of Wilson respecting Prime Numbers, which was first published by Waring in his *Meditationes Analyticae* [32, p. 218], and to which neither himself nor its author could supply the demonstration, excited the attention of the most celebrated analysts of the continent, and to the labors of Lagrange [14] and Euler we are indebted for several modes of proof . . . .

Babbage formulated **Wilson’s theorem** as a criterion for primality: an integer \( p > 1 \) is a prime if and only if \( (p-1)! \equiv -1 \pmod{p} \). (For a modern proof, see Moll [20, p. 66].) He then introduced several such criteria, involving congruences for binomial coefficients (see Granville [11, Sections 1 and 4]). However, some of his claims were unproven or even wrong (as Dubbey points out in [7, pp. 139–141]). One of his valid results is a necessary and sufficient condition for primality, based on a number of simultaneous congruences. Henceforth let \( n \) denote an integer.

**Theorem 1 (Babbage’s Primality Test).** An integer \( p > 1 \) is a prime if and only if

\[
\binom{p+n}{n} \equiv 1 \pmod{p} \tag{1}
\]

for all \( n \) satisfying \( 0 \leq n \leq p-1 \).

This is of only theoretical interest, the test being slower than trial division.

The “only if” part is an immediate consequence of the beautiful **Theorem of Lucas** [15] (see [8, 11, 17, 19] and [20, p. 70]), which asserts that if \( p \) is a prime and the non-negative integers \( a = \alpha_0 + \alpha_1 p + \cdots + \alpha_r p^r \) and \( b = \beta_0 + \beta_1 p + \cdots + \beta_r p^r \) are written in base \( p \) (so that \( 0 \leq \alpha_i, \beta_i \leq p-1 \) for all \( i \)), then

\[
\frac{a}{b} \equiv \prod_{i=0}^{r} \binom{\alpha_i}{\beta_i} \pmod{p}. \tag{2}
\]

(Here the convention is that \( \binom{\alpha}{\beta} = 0 \) if \( \alpha < \beta \).) The congruence (1) follows if \( 0 \leq n \leq p-1 \), for then all the binomial coefficients formed on the right-hand side of (2) are of the form \( \binom{\alpha}{\beta} = 1 \), except the last one, which is \( \binom{1}{0} = 1 \).

However, the theorem was not available to Babbage, because when it was published in 1878 he had been dead for seven years.

Lucas’s theorem implies more generally that for \( p \) a prime and \( m \) a power of \( p \), the congruences

\[
\binom{m+n}{n} \equiv 1 \pmod{p} \quad (0 \leq n \leq m-1) \tag{3}
\]

hold. A converse was proven in 2013: **Meštrović’s theorem** [19] states that if \( m > 1 \) and \( p > 1 \) are integers such that (3) holds, then \( p \) is a prime and \( m \) is a power of \( p \). To begin the proof, Meštrović noted that for \( n = 1 \) the hypothesis gives

\[
\binom{m+1}{1} = m+1 \equiv 1 \pmod{p} \quad \implies \quad p \mid m.
\]
The rest of the proof involves combinatorial congruences modulo prime powers.

As Meštrović pointed out, “the ‘if’ part of Theorem 1 is an immediate consequence of [his theorem] (supposing a priori [that \( m = p \]). Accordingly, [his theorem] may be considered as a generalization of Babbage’s criterion for primality.”

Here we offer another generalization of Babbage’s primality test.

**Theorem 2 (Least-Prime-Factor Test).** The least prime factor of an integer \( m > 1 \) is the smallest natural number \( \ell \) satisfying

\[
\binom{m + \ell}{\ell} \not\equiv 1 \pmod{m}.
\]

For that value of \( \ell \), the least non-negative residue of \( \binom{m + \ell}{\ell} \) modulo \( m \) is \( \frac{m}{\ell} + 1 \).

The proof is given in Section 2.

Babbage’s primality test is an easy corollary of the least-prime-factor test. Indeed, Theorem 2 implies a sharp version of Theorem 1 noticed by Granville in 1995.

**Corollary 1 (Sharp Babbage Primality Test).** Theorem 1 remains true if the range for \( n \) is shortened to \( 0 \leq n \leq \sqrt{p} \).

**Proof.** An integer \( m > 1 \) is a prime if and only if its least prime factor \( \ell \) exceeds \( \sqrt{m} \). The corollary follows by setting \( m = p \) in Theorem 2.

To see that Corollary 1 is sharp in that the range for \( n \) cannot be further shortened to \( 0 \leq n \leq \sqrt{p} - 1 \), let \( q \) be any prime and set \( p = q^2 \). Then \( p \) is not a prime, but the least-prime-factor test with \( m = p \) and \( \ell = q \) implies (1) when \( 0 \leq n \leq q - 1 \).

**Problem 1.** Since the “if” part of Babbage’s primality test is a consequence both of Meštrović’s theorem and of the least-prime-factor test, one may ask, *Is there a common generalization of Meštrović’s theorem and Theorem 2?*

(Note, though, that the modulus in the former is \( p \), while that in the latter is \( m \).)

Actually, the incongruence (1) holds more generally if the least prime factor \( \ell \mid m \) is replaced with any prime factor \( p \mid m \). The following extension of the least-prime-factor test is proven in Section 2. See also Sondow in 2011 Part (a).

**Theorem 3.** (i) Given a positive integer \( m \) and a prime factor \( p \mid m \), we have

\[
\binom{m + p}{p} \not\equiv 1 \pmod{m}.
\]

(ii) If in addition \( p^r \mid m \) but \( p^{r+1} \nmid m \), where \( r \geq 1 \), then

\[
\binom{m + p}{p} \equiv \frac{m}{p} + 1 \not\equiv 1 \pmod{p^r}.
\]
Part (i) is clearly equivalent to the statement that if \( d > 1 \) divides \( m \) and
\[
\binom{m+d}{d} \equiv 1 \pmod{m},
\]
then \( d \) is composite. As an example, for \( m = 260 \) and \( d = 10 \) we have
\[
\binom{270}{10} = 479322759878148681 \equiv 1 \pmod{260}.
\]

The sequence of integers \( m > 1 \), for which some integer \( d \) (necessarily composite) satisfies
\[
d > 1, \quad d \mid m, \quad \binom{m+d}{d} \equiv 1 \pmod{m},
\]
begins [28, Seq. A290040]
\[
m = 260, 1056, 1060, 3460, 3905, 4428, 5000, 5060, 5512, 5860, 6372, 6596, \ldots
\]
and the sequence of smallest such divisors \( d \) is, respectively, [28, Seq. A290041]
\[
d = 10, 264, 10, 10, 55, 18, 20, 10, 52, 10, 18, 34, \ldots
\]

**Problem 2.** Does Theorem 3 extend to prime power factors, i.e., does (5) also hold when \( p \) is replaced with \( p^k \), where \( p^k \mid m \) and \( k > 1 \)? In particular, in the sequence (8), is any term \( d \) a prime power?

See [29, Part (c)].

Babbage also claimed a necessary and sufficient condition for primality based on a single congruence. But he proved only necessity, so we call it a test for non-primality.

**Theorem 4 (Babbage’s Non-Primality Test).** An integer \( m \geq 3 \) is composite if
\[
\binom{2m-1}{m-1} \not\equiv 1 \pmod{m^2}.
\]

Our version of his proof is given in Section 3.

Not only did Babbage not prove the claimed converse, but in fact it is false. Indeed, the numbers \( m_1 = p_1^2 = 283686649 \) and \( m_2 = p_2^2 = 4514260853041 \) are composite but do not satisfy (9), where \( p_1 = 16843 \) and \( p_2 = 2124679 \) are primes.

Here \( p_1 \) (indicated by Selfridge and Pollack in 1964) and \( p_2 \) (discovered by Crandall, Ernvall and Metsänkylä in 1993) are Wolstenholme primes, so called by McIntosh [16] because, while Wolstenholme’s theorem [33] (see [11, 18, 33] and [20, p. 73]) of 1862 guarantees that every prime \( p \geq 5 \) satisfies
\[
\binom{2p-1}{p-1} \equiv 1 \pmod{p^3},
\]

in fact $p_1$ and $p_2$ satisfy the congruence in (10) modulo $p^4$, not just $p^3$ (see Guy [12, p. 131] and Ribenboim [25, p. 23]).

Note that (10) strengthens Babbage’s non-primality test, as Theorem 4 is equivalent to the statement that the congruence in (10) holds modulo $p^2$ for any prime $p \geq 3$.

In their solutions to a problem by Segal in the Monthly, Brinkmann [26] and Johnson [27] made Babbage’s and Wolstenholme’s theorems more precise by showing that every prime $p \geq 5$ satisfies the congruences

$$\binom{2p-1}{p-1} \equiv 1 - \frac{2}{3}B_{p-3} \equiv \binom{2p^2-1}{p^2-1} \pmod{p^4},$$

where $B_k$ denotes the $k$th Bernoulli number, a rational number. (See also Gardiner [9] and McIntosh [16].) Thus, a prime $p \geq 5$ is a Wolstenholme prime if and only if $B_{p-3} \equiv 0 \pmod{p}$. (The congruence means that $p$ divides the numerator of $B_{p-3}$.) In that case, the square of that prime, say $m = p^2$, is composite but must satisfy

$$\binom{2m-1}{m-1} \equiv 1 \pmod{m^2},$$

thereby providing a counterexample to the converse of Babbage’s non-primality test.

Johnson [27] commented that “interest in [Wolstenholme primes] arises from the fact that in 1857, Kummer proved that the first case of [Fermat’s Last Theorem] is true for all prime exponents $p$ such that $p \nmid B_{p-3}$.”

We have seen that the converse of Babbage’s non-primality test is false. The converse of Wolstenholme’s theorem is the statement that if $p \geq 5$ is composite, then (10) does not hold. It is not known whether this is generally true. A proof that it is true for even positive integers was outlined by Trevisan and Weber [30] in 2001. In Section 3, we fill in some details omitted from their argument and extend it to prove the following stronger result.

**Theorem 5 (Converse of Babbage’s Non-Primality Test for Even Numbers).** If a positive integer $m$ is even, then

$$\binom{2m-1}{m-1} \not\equiv 1 \pmod{m^2}. \quad (11)$$

2 Proofs of the least-prime-factor test and its extension

We prove Theorems 2 and 3. The arguments use only mathematics available in Babbage’s time.
Proof (Theorem 3). As $\ell$ is the smallest prime factor of $m$, if $0 < k < \ell$ then $k!$ and $m$ are coprime. In that case, Bézout’s identity (proven in 1624 by Bachet in a book with the charming title Pleasant and Delectable Problems [3, p. 18, Proposition XVIII]—see [6, Section 4.3]) gives integers $a$ and $b$ with $ak! + bm = 1$. Multiplying Bézout’s equation by the number $(\binom{m}{k} = m(m-1) \cdots (m-k+1)/k)!$ yields
\[ am(m-1) \cdots (m-k+1) + bm \binom{m}{k} = \binom{m}{k}, \]
so $(\binom{m}{k}) \equiv 0 \pmod{m}$ if $1 \leq k \leq \ell - 1$. Now, for $n = 0, 1, \ldots, \ell - 1$, Vandermonde’s convolution [31] (see [20, p. 164]) of 1772 gives
\[ \binom{m+n}{n} = \sum_{k=0}^{n} \binom{m}{k} \binom{n}{n-k} \equiv \binom{m}{0} \binom{n}{n} \pmod{m}. \]
(To see the equality, equate the coefficients of $x^n$ in the expansions of $(1+x)^{m+n}$ and $(1+x)^m(1+x)^n$.) Thus, we arrive at the congruences
\[ \binom{m+n}{n} \equiv 1 \pmod{m} \quad (0 \leq n \leq \ell - 1). \quad (12) \]

On the other hand, from the identity
\[ \binom{a}{b} = \binom{a}{b} \binom{a-1}{b-1} \quad (13) \]
(to prove it, use factorials), the congruence (12) for $n = \ell - 1$, the integrality of $\frac{m+\ell}{\ell} = \frac{m}{\ell} + 1$, and the inequality $\ell > 1$ (as $\ell$ is a prime), we deduce that
\[ \binom{m+\ell}{\ell} = \frac{m+\ell}{\ell} \binom{m+\ell-1}{\ell-1} \equiv \frac{m}{\ell} + 1 \not\equiv 1 \pmod{m}. \]
Together with (12), this implies the least-prime-factor test. \hfill \qed

Proof (Theorem 4). It suffices to prove (ii). Set
\[ g \overset{\text{def}}{=} \gcd((p-1)!, m) \quad \text{and} \quad m_p \overset{\text{def}}{=} \frac{m}{g}. \]
Note that
\[ p \text{ prime } \implies p \nmid g \implies p^r \mid m_p, \quad (14) \]
since $p^r \mid m$. Bézout’s identity gives integers $a$ and $b$ with $a(p-1)! + bm = g$. When $0 < k < p$, multiplying Bézout’s equation by $\binom{m}{k}$ yields
\[ am(m-1) \cdots (m-k+1) \frac{(p-1)!}{k!} + bm \binom{m}{k} = g \binom{m}{k}. \]
with \((p - 1)!/k!\) an integer, so \(g(m) \equiv 0 \pmod{m}\). Dividing by \(g\) gives

\[
\left(\frac{m}{k}\right) \equiv 0 \pmod{m_p} \quad (1 \leq k \leq p - 1).
\]

Combining this with (13) and Vandermonde’s convolution, we get

\[
\binom{m + p}{p} = \frac{m + p}{p} \binom{m + p - 1}{p - 1} = \frac{m + p}{p} \sum_{k=0}^{p-1} \left(\frac{m}{k}\right) \left(\frac{p - 1}{p - 1 - k}\right) \equiv \frac{m}{p} + 1 \pmod{m_p}.
\]

As \(p^{r+1} \nmid m\), we have \(p^r \nmid \frac{m}{p}\). Now, (14) and (15) imply (6), as required.

3 Proofs of Babbage’s non-primality test and its converse for even numbers

The following proof is close to the one Babbage gave.

**Proof (Theorem 4).** Suppose on the contrary that \(m\) is prime. If we have

\[
1 \leq n \leq m - 1,
\]

then \(m\) divides the numerator of \(\binom{m}{n} = m!/n!(m - n)\) but not the denominator, so \(\binom{m}{n} \equiv 0 \pmod{m}\). Thus, by (13) and a famous case of Vandermonde’s convolution,

\[
2^{m - 1} = 2^{m} = \sum_{n=0}^{m} \binom{m}{n}^2 \equiv 1^2 + 1^2 \equiv 2 \pmod{m^2}.
\]

But as \(m \geq 3\) is odd, \(\binom{m}{n}\) contradicts (0). Therefore, \(m\) is composite.

Before giving the proof of Theorem 5, we establish two lemmas. For any positive integer \(k\), let \(2^{v(k)}\) denote the highest power of 2 that divides \(k\).

**Lemma 1.** If \(m \geq n \geq 1\) are integers satisfying \(n \leq 2^{v(m)}\), then the formula \(v(\binom{m}{n}) = v(m) - v(n)\) holds.

**Proof.** Let \(m = 2^r m'\) with \(m'\) odd. Note that \(v(2^r m' - k) = v(k)\) if \(0 < k < 2^r\).

(Proof. Write \(k = 2^t k'\), where \(0 \leq t = v(k) \leq r - 1\) and \(k'\) is odd. Then \(2^{r-t} m' - k'\) is also odd, so \(v(2^r m' - k) = v(2^t(2^{r-t} m' - k')) = t = v(k)\).) The logarithmic formula \(v(ab) = v(a) + v(b)\) then implies that when \(1 \leq n \leq 2^r\) the exponent of the highest power of 2 that divides the product

\[
n! \binom{m}{n} = 2^r m'(2^r m' - 1)(2^r m' - 2) \cdots (2^r m' - (n - 1))
\]

is \(v(n!) + v(\binom{m}{n}) = r + v(1 \cdot 2 \cdots (n - 1))\), so \(v(\binom{m}{n}) = r - v(n)\). As \(r = v(m)\), this proves the desired formula.
Lemma 1 is sharp in that the hypothesis $n \leq 2^v(m)$ cannot be replaced with the weaker hypothesis $v(n) \leq v(m)$. For example, $v\left(\begin{pmatrix}10 \\ 6\end{pmatrix}\right) = v(210) = 1$, but $v(10) - v(6) = 0$.

**Lemma 2.** A binomial coefficient $\binom{2^m-1}{m-1}$ is odd if and only if $m = 2^r$ for some $r \geq 0$.

**Proof.** Kummer’s theorem [13] (see [20, p. 78] or [24]) for the prime 2 states that $v\left(\binom{a+b}{a}\right)$ equals the number of carries when adding $a$ and $b$ in base 2 arithmetic. Hence $v\left(\binom{m+m}{m}\right)$ is the number of ones in the binary expansion of $m$, and so $v\left(\binom{2^m}{m}\right) = 1$ if and only if $m = 2^r$ for some $r \geq 0$. As $\binom{2^m}{m} = 2\binom{2^m-1}{m-1}$ by (13), we are done.

We can now prove the converse of Babbage’s non-primality test for even numbers.

**Proof (Theorem 5).** For $m \geq 2$ not a power of 2, Lemma 2 implies that $\binom{2^m-1}{m-1}$ is even, so $\binom{2^m-1}{m-1}$ is congruent modulo 4 to either 0 or 2. For $m \geq 2$ a power of 2, say $m = 2^r$, the equalities in (16) and the symmetry $\binom{m}{n} = \binom{m}{m-n}$ yield

$$\binom{2^m-1}{m-1} = 1 + \frac{1}{2} \binom{2^r-1}{2^r-1}^2 + \sum_{k=1}^{2^r-1} \binom{2^r}{k}^2,$$

and Lemma 1 implies that $\frac{1}{2} \binom{2^r-1}{2^r-1}^2 \equiv 2(\text{mod } 4)$ and that $\binom{2^r}{k}^2 \equiv 0(\text{mod } 4)$ when $0 < k < 2^r - 1$; thus, by addition $\binom{2^m-1}{m-1} \equiv 3(\text{mod } 4)$. Hence for all $m \geq 2$ we have $\binom{2^m-1}{m-1} \not\equiv 1(\text{mod } 4)$. Now as 4 divides $m^2$ when $m$ is even, (11) holds a fortiori. This completes the proof.

References

1. C. Babbage, Demonstration of a theorem relating to prime numbers, Edinburgh Phil. J. 1, 46–49 (1819); available at [http://books.google.com/books?id=KrA-AAAAYAAJ&pg=PA46](http://books.google.com/books?id=KrA-AAAAYAAJ&pg=PA46)
2. C. Babbage, *Passages from the Life of a Philosopher* (Longman, Green, Longman, Roberts, & Green, London, 1864); available at [http://djm.cc/library/Passages_of_a_Philosopher_Babbage_edited.pdf](http://djm.cc/library/Passages_of_a_Philosopher_Babbage_edited.pdf)
3. C. G. Bachet, *Problèmes plaisants et délectables, qui se font par les nombres*, 2nd edn. (Rigaud, Lyon, 1624); available at [http://bsb3.bsb.lrz.de/~db/1008/bsb10081407/images/bsb10081407_00036](http://bsb3.bsb.lrz.de/~db/1008/bsb10081407/images/bsb10081407_00036)
4. W. A. Beyer, review of [7], Am. Math. Mon. 86, 66–67 (1979)
5. B. D. Blackwood, Charles Babbage. In: D. R. Franceschetti (ed) *Biographical Encyclopedia of Mathematicians*. (Cavendish, New York, 1998), pp. 33–36; available at [http://www.blackwood.org/Babbage.htm](http://www.blackwood.org/Babbage.htm)
Extending Babbage’s (Non-)Primality Tests

6. E. Barbin, J. Borowczyk, J.-L. Chabert, A. Djebbar, M. Guillemot, J.-C. Martzloff, and A. Michel-Pajus, *A History of Algorithms: From the Pebble to the Microchip*. J.-L. Chabert (ed). Trans. by C. Weeks (Springer, Berlin and Heidelberg, 2012)

7. J. M. Dubbey, *The Mathematical Work of Charles Babbage* (Cambridge Univ. Press, Cambridge, 1978)

8. N. J. Fine, Binomial coefficients modulo a prime, Am. Math. Mon. 54, 589–592 (1947)

9. A. Gardiner, Four problems on prime power divisibility, Am. Math. Mon. 95, 926–931 (1988)

10. J. Grabiner, review of From Newton to Hawking: A History of Cambridge University’s Lucasian Professors of Mathematics by K. C. Knox and R. Noakes, Am. Math. Mon. 112, 757–762 (2005)

11. A. Granville, Arithmetic properties of binomial coefficients I: Binomial coefficients modulo prime powers. In: J. Borwein (ed), *Organic mathematics* (Burnaby, BC, 1995). CMS Conf. Proc. Vol. 20 (American Mathematical Society, Providence, RI, 1997), pp. 253–275; available at http://www.dms.umontreal.ca/~andrew/PDF/BinCoeff

12. R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edn. (Springer, New York, 2004)

13. E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, J. Reine Angew. Math. 44, 93–146 (1852)

14. J. L. Lagrange, Démonstration d’un théorème nouveau concernant les nombres premiers, Nouv. Mém. Acad. Roy. Sci. Belles-Lettres, Berlin 2, 125–137 (1771); available at https://books.google.com/books?id=UAAAAAAJ&amp;pg=PA125

15. É. Lucas, Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier, Bull. Soc. Math. France 6, 49–54 (1878); available at http://archive.numdam.org/ARCHIVE/BSMF/BSMF_1878__6_/BSMF_1878__6__49_1/BSMF_1878__6__49_1.pdf

16. R. J. McIntosh, On the converse of Wolstenholme’s theorem, Acta Arith. 71, 381–389 (1995)

17. R. Meštrović, A note on the congruence \( \binom{nd}{md} \equiv \binom{n}{m} \); Am. Math. Mon. 116, 75–77 (2009)

18. R. Meštrović, Wolstenholme’s theorem: Its generalizations and extensions in the last hundred and fifty years (1862–2011), arXiv:1111.3057 [math.NT] (2011); available at http://arxiv.org/abs/1111.3057

19. R. Meštrović, An extension of Babbage’s criterion for primality, Math. Slovaca 63, 1179–1182 (2013); available at http://dx.doi.org/10.2478/s12175-013-0164-8

20. V. H. Moll, *Numbers and Functions: From a Classical-Experimental Mathematician’s Point of View*. Student Mathematical Library, Vol. 65 (American Mathematical Society, Providence, RI, 2012)

21. M. Moseley, *Irascible Genius: A Life of Charles Babbage, Inventor* (Hutchinson, London, 1964)

22. J. J. O’Connor and E. F. Robertson, Charles Babbage, MacTutor History of Mathematics, http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Babbage.html

23. J. T. O’Donnell, review of *Charles Babbage: Pioneer of the Computer* by A. Hyman, Am. Math. Mon. 92, 522–525 (1985)

24. C. Pomerance, Divisors of the middle binomial coefficient, Am. Math. Mon. 122, 636–644 (2015)

25. P. Ribenboim, *The Little Book of Bigger Primes* (Springer-Verlag, New York, 2004)

26. D. Segal and H. W. Brinkmann, E435, Am. Math. Mon. 48, 269–271 (1941)

27. D. Segal and W. Johnson, E435, Am. Math. Mon. 83, 813 (1976)
28. N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences. Published electronically at [http://oeis.org/](http://oeis.org/)(2018)

29. J. Sondow, Problem 12030, Am. Math. Mon. 125, 276 (2018)

30. V. Trevisan and K. Weber, Testing the converse of Wolstenholme’s theorem, Mat. Contemp. 21, 275–286 (2001)

31. A.-T. Vandermonde, Mémoire sur des irrationnelles de différents ordres, avec une application au cercle, Mém. Acad. Roy. Sci. Paris (1772), 489–498; available at [http://gallica.bnf.fr/ark:/12148/bpt6k3570q/f79](http://gallica.bnf.fr/ark:/12148/bpt6k3570q/f79)

32. E. Waring, *Meditationes Algebraicae* (Cambridge Univ. Press, Cambridge, 1770)

33. J. Wolstenholme, On certain properties of prime numbers, Q. J. Pure Appl. Math. 5, 35–39 (1862); available at [http://books.google.com/books?id=vLOKAAAAIAAJ&pg=PA35](http://books.google.com/books?id=vLOKAAAAIAAJ&pg=PA35)