VERSITA

Mathematica Slovaca

DOI: 10.2478/s12175-013-0164-8
Math. Slovaca **63** (2013), No. 6, 1179–1182

AN EXTENSION OF BABBAGE'S CRITERION FOR PRIMALITY

Romeo Meštrović

(*Communicated by Jörg Brüdern*)

ABSTRACT. Let $n > 1$ and $k > 1$ be positive integers. We show that if

$$\binom{n+m}{n} \equiv 1 \pmod{k}$$

for each integer m with $0 \leq m \leq n-1$, then k is a prime and n is a power of this prime. In particular, this assertion under the hypothesis that $n = k$ implies that n is a prime. This was proved by Babbage, and thus our result may be considered as a generalization of this criterion for primality.

1. Introduction

Gauss ([2: art. 329]) wrote:

> *The problem of distinguishing prime numbers from composite numbers . . . is known to be one of the most important and useful in arithmetic. . . . The dignity of the science itself seems to require that every possible means be explored for solution of a problem so elegant and so celebrated.*

As far back as 1819 (see [3]), Charles Babbage gave an easily proved characterization of the primes, based on a number of simultaneous congruences:

Theorem 1.1. *An integer $n \geq 2$ is a prime if and only if*

$$\binom{n+m}{n} \equiv 1 \pmod{n} \tag{1}$$

for all positive integers m with $0 \leq m \leq n-1$.

A beautiful *theorem of Lucas* ([4]; also see [3]) states that for every prime p,

$$\binom{n}{m} \equiv \prod_{i=0}^{s} \binom{n_i}{m_i} \pmod{p}. \tag{2}$$

2010 Mathematics Subject Classification: Primary 11B65, 11A07.
Keywords: Babbage's criterion for primality, Lucas' theorem, congruence, prime power.

(with the convention that $\binom{a}{b} = 0$ if $a < b$), where $n = n_0 + n_1 p + \cdots + n_s p^s$ and $m = m_0 + m_1 p + \cdots + m_s p^s$ are the *p-adic expansions* of nonnegative integers n and m (so that $0 \leq m_i, n_i \leq p-1$ for each i). Note that for any positive integer $e \geq 1$ the congruence (2) immediately yields

$$\binom{np^e}{mp^e} \equiv \binom{n}{m} \pmod{p}, \tag{3}$$

since the same products of binomial coefficients are formed on the right side of (2), in both cases, other than extra $\binom{0}{0} = 1$.

Also, by Lucas' theorem, for any prime p and positive integers e and m such that $0 \leq m \leq p^e - 1$, we have

$$\binom{p^e + m}{p^e} \equiv 1 \pmod{p}. \tag{4}$$

In particular, the above congruence with $e = 1$ yields (1) for a prime $n = p$ and for $0 \leq m \leq p-1$. In this paper we prove a converse statement related to the congruence (4) as follows.

Theorem 1.2. *Let $n > 1$ and $k > 1$ be positive integers such that*

$$\binom{n+m}{n} \equiv 1 \pmod{k} \tag{5}$$

for each integer m with $0 \leq m \leq n-1$. Then k is a prime and n is a power of this prime.

Remark 1. Note that the "if" part of Theorem 1.1 is an immediate consequence of Theorem 1.2 (supposing apriori that $n = k$). Accordingly, Theorem 1.2 may be considered as a generalization of Babbage's criterion for primality given by Theorem 1.1.

Remark 2. Recently ([5: Theorem, p. 75]), in terms of a number of simultaneous binomial congruences, it is proved a criterion for two positive integers to be powers of the same prime.

2. Proof of Theorem 1.2

Besides Lucas type congruences (3) and (4) given before, for the proof of Theorem 1.2, we need the following result.

Lemma 2.1. *Let p be any prime, and let e be an arbitrary positive integer. Then we have the congruence*

$$\binom{p^e + p^{e-1}}{p^e} \equiv p + 1 \pmod{p^2}. \tag{6}$$

P r o o f. By a result of W. Ljunggren ([1]; also see [3]),

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3}, \tag{7}$$

for any integers $n \geq m \geq 1$ and a prime $p \geq 5$. Consequently, if $p \geq 5$ is a prime, then (7) with $n = p^{e-1} + p^{e-2}$, $m = p^{e-1}$ and any integer $e \geq 2$ yields

$$\binom{p^e + p^{e-1}}{p^e} \equiv \binom{p^{e-1} + p^{e-2}}{p^{e-1}} \pmod{p^3},$$

whence (6) follows by induction on $e \geq 1$ (for $e = 1$ (6) reduces to the identity).

Further, by [6: (3.2) of Lemma 3.2], $\binom{3n}{3m} \equiv \binom{n}{m} \pmod{3^2}$. As in the previous case, this congruence yields

$$\binom{3^e + 3^{e-1}}{3^e} \equiv 4 \pmod{3^2}.$$

Finally, by [6: (3.3) of Lemma 3.2], we immediately have

$$\binom{2n}{2m} \equiv (-1)^m \binom{n}{m} \pmod{2^{2\mathrm{ord}_2(n)}}.$$

Applying the above congruence $e - 2$ times, we find that

$$\begin{aligned} \binom{3 \cdot 2^{e-1}}{2 \cdot 2^{e-1}} &\equiv (-1)^{2^{e-1}} \binom{3 \cdot 2^{e-2}}{2 \cdot 2^{e-2}} \equiv \dots \\ &\equiv (-1)^{2^2} \binom{3 \cdot 2}{2^2} \equiv 7 \pmod{8}, \end{aligned}$$

whence we see that (6) holds for $p = 2$. This completes the proof. □

P r o o f o f T h e o r e m 1.2. By the assumption, for $m = 1$ we have

$$\binom{n+1}{n} = n + 1 \equiv 1 \pmod{k}, \tag{8}$$

whence we see that $k \mid n$.

Suppose that n is not a prime power. Because of $k > 1$ we can choose a prime q such that $q \mid k$. Since $k \mid n$, we may write $n = q^f l$ where f and l are positive integers and l coprime to q. Since n is not a prime power, we also know that $l > 1$. By the congruence (3) with $m = q^f < n$, we find that

$$\binom{n+m}{n} = \binom{q^f(l+1)}{q^f l} \equiv \binom{l+1}{l} = l + 1 \not\equiv 1 \pmod{q}.$$

However, in view of the fact that $q \mid k$, by (5) must be

$$\binom{n+m}{n} \equiv 1 \pmod{q}.$$

This contradicts the previous congruence. Hence, n is a prime power, that is, $n = q^f$ with a prime q and $f \geq 1$. From this and the fact that $k \mid n$ it follows that $k = q^s$ with $1 \leq s \leq f$. By (6) of Lemma 2.1, we have

$$\binom{q^f + q^{f-1}}{q^f} \equiv q + 1 \pmod{q^2}. \tag{9}$$

On the other hand, if we suppose that $s \geq 2$, the assumption (5) of Theorem 1.2 for $m = q^{f-1}$ gives

$$\binom{q^f + q^{f-1}}{q^f} \equiv 1 \pmod{q^s} \equiv 1 \pmod{q^2}.$$

The above congruence and (9) yield $q^2 \mid q$. A contradiction, and hence must be $s = 1$, that is, $k = q$ is a prime, and the theorem is proved. □

Remark 3. We see from the proof of Theorem 1.2 that the range for m may be shortened only to $0 \leq m \leq n/2$. This is immediate from the fact that in this proof we have put $m = q^f$ and so, $n = q^f l = ml \geq 2m$ because of the assumption that $l > 1$. Recall that under the "Babbage's assumption" from Theorem 1.1 that $n = k$, A. Granville [3] noticed that this range for m may be shortened to $0 \leq m \leq \sqrt{n}$.

Acknowledgement. The author gratefully acknowledges valuable suggestions from the anonymous referees.

REFERENCES

[1] BRUN, V. — STUBBAN, J. O. — FJELDSTAD, J. E. — TAMBS LYCHE, R — AUBERT, K. E. — LJUNGGREN, W — JACOBSTHAL, E.: *On the divisibility of the difference between two binomial coefficients*. In: Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949, Johan Grundt Tanums Forlag, Oslo, 1952, pp. 42–54.

[2] GAUSS, C. F.: *Disquisitiones Arithmeticae*, Fleischer, Leipzig, 1801.

[3] GRANVILLE, A.: *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, pp. 253–276.

[4] LUCAS, E.: *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France **6** (1877-1878), 49–54.

[5] MEŠTROVIĆ, R.: *A Note on the Congruence* $\binom{nd}{md} \equiv \binom{n}{m} \pmod{q}$, Amer. Math. Monthly **116** (2009), 75–77.

[6] SUN, Z. W.—DAVIS, D. M.: *Combinatorial congruences modulo prime powers*, Trans. Amer. Math. Soc. **359** (2007), 5525–5553; `http://arxiv.org/abs/math.NT/0508087v5`.

Received 14. 7. 2011
Accepted 16. 11. 2011

Maritime Faculty
University of Montenegro
Dobrota 36
85330 Kotor
MONTENEGRO
E-mail: romeo@ac.me