



Exactly When Is $(a + b)^n \equiv a^n + b^n \pmod{n}$?

Author(s): Pratibha Ghatage and Brian Scott

Source: *The College Mathematics Journal*, Vol. 36, No. 4 (Sep., 2005), p. 322

Published by: Mathematical Association of America

Stable URL: <http://www.jstor.org/stable/30044877>

Accessed: 24/03/2010 21:22

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 service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. 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 College Mathematics Journal*.

<http://www.jstor.org>

Exactly When Is $(a + b)^n \equiv a^n + b^n \pmod{n}$?

Pratibha Ghatage (p.ghatage@csuohio.edu) and Brian Scott (b.scott@csuohio.edu),
Cleveland State University, Cleveland, OH 44115

When this question was asked on a test in abstract algebra, most of the class conjectured that it was true exactly when n is prime. The correct answer (to our pleasant surprise) involves Fermat's little theorem. It is well known that if n is prime, the result is true. The standard proof is based on the following lemma, which is a simple exercise.

Lemma 1. *A natural number n divides*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

whenever $0 < k < n$, if and only if n is prime.

Corollary. *If n is prime, then $(a + b)^n \equiv a^n + b^n \pmod{n}$.*

This is a simple application of the binomial theorem [1, p. 9] and we omit the proof.

Now one is tempted to try to prove the converse to the Corollary. But a look at Fermat's little theorem [1, Theorem 5.1, p. 92] suggests another connection.

Proposition. *For a natural number n , the following are equivalent:*

- (1) $(a + b)^n \equiv a^n + b^n \pmod{n}$.
- (2) $x^n \equiv x \pmod{n}$ for all x , i.e., Fermat's little theorem holds for n .

Proof. Suppose that (1) holds. Then the map $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ defined by $f(x) = x^n$ is additive. Clearly $f(1) = 1$; hence, writing $x = 1 + \cdots + 1$, x times over, we see that $f(x) = x$ in \mathbb{Z}_n , i.e., (2) holds.

Conversely, if Fermat's Little Theorem holds for n , then letting $x = a + b$, we see that $(a + b)^n \equiv a + b \pmod{n}$. Also by applying Fermat's little theorem to a and b , we see that $a^n \equiv a \pmod{n}$ and $b^n \equiv b \pmod{n}$. Hence (1) holds. ■

It is well-known that Fermat's little theorem holds for certain composite numbers called Carmichael numbers, and that the smallest Carmichael number is 561. See [1, p. 95].

Thus we know that $(a + b)^n \equiv a^n + b^n \pmod{n}$ holds exactly when n is either prime or a Carmichael number.

Acknowledgment. We are grateful to Underwood Dudley for helpful discussions.

Reference

1. D. M. Burton, *Elementary Number Theory*, 5th ed., McGraw-Hill, 2002.

