Exactly When Is $(a+b)^n \equiv a^n + b^n (\bmod n)$?

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* $(a+b)^n \equiv a^n + b^n (\bmod n)$.

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) $(a+b)^n \equiv a^n + b^n (\bmod n)$.

(2) $x^n \equiv x (\bmod n)$ *for all x, i.e., Fermat's little theorem holds for n.*

Proof. Suppose that (1) holds. Then the map $f : \mathbb{Z}_n \to \mathbb{Z}_n$ 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 $(a+b)^n \equiv a + b$ (mod n). Also by applying Fermat's little theorem to a and b, we see that $a^n \equiv a (\bmod n)$ and $b^n \equiv b (\bmod n)$. 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 $(a+b)^n \equiv a^n + b^n$ (mod 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.