ON CONGRUENCE MODULO *A* POWER OF A PRIME

M. G. MONZINGO
Southern Methodist University, Dallas, Texas 75275

A problem which appears in many textbooks in number theory, e.g. [1], is the following:
If $a^p \equiv b^p \pmod p$, then $a^p \equiv b^p \pmod{p^2}$.
In this paper this result will be generalized to higher powers of the prime p. Also, there will be a generalization to a composite modulus.

Lemma 1. If n is a positive integer for which $a^{p^n} \equiv b^{p^n} \pmod p$, then $a \equiv b \pmod p$.

Proof. Let $n = 1$; then, $a \equiv a^p \equiv b^p \equiv b \pmod p$ by Fermat's Theorem. Suppose that $a^{p^k} \equiv b^{p^k} \pmod p$ implies that $a \equiv b \pmod p$. If $a^{p^{k+1}} \equiv b^{p^{k+1}} \pmod p$, then $(a^{p^k})^p \equiv (b^{p^k})^p \pmod p$. Hence,

$$a^{p^k} \equiv (a^{p^k})^p \equiv (b^{p^k})^p \equiv b^{p^k} \pmod p$$

by Fermat's Theorem. By the induction hypothesis, $a \equiv b \pmod p$.

Lemma 2. If $a^{p^n} \equiv b^{p^n} \pmod{p^n}$, then

$$p^n \mid (a^{p^n-1} + a^{p^n-2}b + \cdots + b^{p^n-1}).$$

Proof. By Lemma 1, $p \mid (a - b)$, and, thus, $a = b + tp$ for some integer t. Then, with $d = p^n$,

$$\begin{aligned}
a &= b + (tp)\\
a^2 &= b^2 + 2b(tp) + (tp)^2\\
a^3 &= b^3 + \cdots + (tp)^3\\
&\vdots\\
a^{d-1} &= b^{d-1} + (d-1)b^{d-2}(tp) + \cdots + (tp)^{d-1}.
\end{aligned}$$

By multiplying the i^{th} row by b^{d-i-1}, we obtain:

$$\begin{aligned}
b^{d-1} &= b^{d-1}\\
ab^{d-2} &= b^{d-1} + b^{d-2}(tp)\\
a^2b^{d-3} &= b^{d-1} + 2b^{d-2}(tp) + b^{d-3}(tp)^2\\
&\vdots\\
a^{d-2}b &= b^{d-1} + (d-2)b^{d-2}(tp) + \cdots + b(tp)^{d-2}\\
a^{d-1} &= b^{d-1} + (d-1)b^{d-2}(tp) + \cdots + (tp)^{d-1}.
\end{aligned}$$

The coefficient of $b^{d-k}(tp)^{k-1}$ in the expansion $a^{d-1} + a^{d-2}b + \cdots + b^{d-1}$ is

$$\sum_{i=k-1}^{d-1} \binom{i}{k-1}.$$

Using the identity

$$\binom{b+1}{a} = \binom{b}{a} + \binom{b}{a-1},$$

rewritten as

$$\binom{b}{a-1} = \binom{b+1}{a} - \binom{b}{a},$$

we have

$$\sum_{i=k-1}^{d-1}\binom{i}{k-1} = \sum_{i=k-1}^{d-1}\binom{i+1}{k} - \sum_{i=k-1}^{d-1}\binom{i}{k} = \binom{d}{k} + \sum_{i=k-1}^{d-2}\binom{i+1}{k} - \sum_{i=k}^{d-1}\binom{i}{k} - \binom{k-1}{k}$$

$$= \binom{d}{k} + \sum_{i=k}^{d-1}\binom{i}{k} - \sum_{i=k}^{d-1}\binom{i}{k} - 0 = \binom{d}{k}.$$

This implies that the k^{th} term of $a^{d-1} + \cdots + b^{d-1}$ expressed as a polynomial in (tp) is $(dr/k)b^{d-k}(tp)^{k-1}$, where

$$r = \binom{d-1}{k-1}.$$

If $(p,k) = 1$, then

$$p^n \mid (dr/k)b^{d-k}(tp)^{k-1}$$

since $p^n \mid d$. Suppose that $(p,k) \neq 1$; then, $k = p^m g$, where $m \neq 0$ and $p \nmid g$. To show that $m \leqslant k-1$, suppose to the contrary that $m > k-1$, i.e., $m \geqslant k$. Since $p > 1$, $p^m > m$. Hence, $p^m > m \geqslant k$, a contradiction. Thus, $m < k-1$, and

$$(dr/k)b^{d-k}(tp)^{k-1} = (dr/g)b^{d-k}t^{k-1}p^{k-m-1},$$

where p^{k-m-1} is integral. Since $p \nmid g$,

$$p^n \mid (dr/g)b^{d-k}t^{k-1}p^{k-m-1}.$$

Therefore, p^n divides each term of $a^{d-1} + \cdots + b^{d-1}$ expressed as a polynomial in (tp). The conclusion follows.

The next lemma is a generalization of the problem mentioned at the beginning of this paper.

Lemma 3. If $a^{p^n} \equiv b^{p^n} \pmod{p^n}$, then $a^{p^n} \equiv b^{p^n} \pmod{p^{n+1}}$.

Proof. Let $d = p^n$; then, by Lemma 1, $p \mid (a-b)$, and by Lemma 2, $p^n \mid (a^{d-1} + \cdots + b^{d-1})$. This implies that

$$p^{n+1} \mid (a-b)(a^{d-1} + \cdots + b^{d-1}),$$

i.e., $p^{n+1} \mid (a^{p^n} - b^{p^n})$.

Theorem. If $a^m \equiv b^m \pmod{m}$, then $a^m \equiv b^m \pmod{m \cdot p_1 p_2 \cdots p_r}$, where $p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ is the canonical factorization of m.

Proof. Let $q = m/p_i^{n_i}$; then

$$(a^q)^{p_i^{n_i}} \equiv a^m \equiv b^m \equiv (b^q)^{p_i^{n_i}} \pmod{p_i^{n_i}}.$$

By Lemma 3, $a^m \equiv b^m \pmod{p_i^{n_i+1}}$. The conclusion follows since the p_i are relatively prime.

The following example shows that in general the modulus in Lemma 3 and in the Theorem cannot be increased any more.

Example: $7^9 \equiv 1^9 \pmod{9}$ implies that $7^9 \equiv 1^9 \pmod{27}$, but $7^9 \not\equiv 1^9 \pmod{81}$.

REFERENCE

1. I. Niven and H. Zuckerman, *An Introduction to the Theory of Numbers,* Wiley, New York, 1960.

****