Mixed Exponential and Polynomial Congruences

Stanley Rabinowitz

Rarely in the mathematical literature does one find a divisibility result or a congruence that includes both an exponential term and a polynomial term. For example, for all positive integers $n$,

$$64 \mid (3^{2n+3} + 40n - 27)$$

and

$$3^{2n+5} + 160n^2 \equiv 56n + 243 \pmod{512}$$

which come from chapter 16 of Wolstenholme [2]. It is the purpose of this note to investigate such congruences.

We start with a preliminary result.

**Lemma.** Let $c$, $d$, $k$, and $m$ be integers with $c > 0$, $\gcd(c, m) = 1$, and $\gcd(k, m) = 1$. If there exists a polynomial $f(x)$ of degree $d$ such that for all integers $n \geq 0$,

$$k \cdot c^n \equiv f(n) \pmod{m},$$

then

$$m \mid (c - 1)^{d+1}.$$ 

**Proof.** Suppose such a polynomial $f(x)$ exists. Let $\Delta$ denote the forward difference operator. That is, for any function $h(n)$,

$$\Delta h(n) = h(n + 1) - h(n).$$

Let $\Delta^d$ represent a $d$-fold repetition of $\Delta$. It is well known (Boole [1]) or easily shown by induction that

$$\Delta k f(n) = k \Delta f(n),$$

$$\Delta^d c^n = c^{n-d} (c-1)^d,$$

and

$$\Delta^{d+1} f(n) = 0 \quad \text{if} \quad \deg f = d.$$ 

Applying the difference operator $d + 1$ times in succession to the equation $k \cdot c^n \equiv f(n) \pmod{m}$ yields

$$k \cdot c^{n-d-1} (c-1)^{d+1} \equiv 0 \pmod{m},$$
or \( m \mid k \cdot c^{n-d-1}(c-1)^{d+1} \). But since \( \gcd(m, c) = 1 \) and \( \gcd(m, k) = 1 \), we must have \( m \mid (c-1)^{d+1} \) as required.

Now we can state our result in more generality.

**Theorem 1.** Let \( a, b, c, d, k, \) and \( m \) be integers with \( a > 0, c > 0, \gcd(c, m) = 1, \) and \( \gcd(k, m) = 1 \). If there exists a polynomial \( f(x) \) of degree \( d \) such that for all integers \( n \geq 0 \),

\[
k \cdot c^{an+b} \equiv f(n) \pmod{m},
\]

then

\[
m \mid (c^{a} - 1)^{d+1}.
\]

**Proof.** Replace \( c \) by \( c^a \) is our lemma, noting that if \( \gcd(c^a, m) = 1 \), then \( \gcd(c, m) = 1 \). Also, replace \( k \) by \( k \cdot c^b \), noting that if \( \gcd(k, m) = 1 \) and \( \gcd(c, m) = 1 \), then \( \gcd(k \cdot c^b, m) = 1 \). This gives us Theorem 1.

We can also prove the converse.

**Theorem 2.** Let \( a, b, c, d, k, \) and \( m \) be positive integers such that

\[
m \mid (c^{a} - 1)^{d+1}.
\]

Then there exists a polynomial \( f(x) \) of degree at most \( d \) such that for all integers \( n \geq 0 \),

\[
k \cdot c^{an+b} \equiv f(n) \pmod{m}.
\]

In particular, one such polynomial is

\[
f(x) = \sum_{j=0}^{d} \binom{x}{j} k c^b (c^a - 1)^j. \quad (*)
\]

**Proof.** By the Binomial Theorem, we have

\[
(y + 1)^n = \sum_{j=0}^{n} \binom{n}{j} y^j.
\]

Let \( y = c^a - 1 \) and note that every term involving \( y^j \) where \( j > d \) is divisible by \( y^{d+1} = (c^a - 1)^{d+1} \) and thus is also divisible by \( m \) by our hypothesis that \( m\mid(c^{a} - 1)^{d+1} \). Thus, these terms are congruent to 0 modulo \( m \), and we are left with

\[
(y + 1)^n \equiv \sum_{j=0}^{d} \binom{n}{j} y^j \pmod{m},
\]

or

\[
c^{an} \equiv \sum_{j=0}^{d} \binom{n}{j} (c^a - 1)^j \pmod{m}.
\]
Multiplying both sides by \( k \cdot c^b \) shows that (*) is indeed the desired polynomial function of degree at most \( d \).

Note that the function \( f \) is not unique; there may be other polynomial functions of degree \( d \) meeting the given conditions. Note also that if \( m \mid (c^a - 1)^{d+1} \), then it is not hard to show that \( c \) and \( m \) are relatively prime. Note also that the polynomial \( f \) that we found has degree exactly \( d \) if \( \gcd(k, m) = 1 \) and \( m \) does not divide \( (c^a - 1)^d \).

**Examples.**

Now that we have our general results, we can crank out interesting examples. Here are but just a few.

\[
\begin{align*}
29^{2n} & \equiv 140n + 1 \pmod{700}, \\
2002^n & \equiv 138n + 1 \pmod{207}, \\
11^n & \equiv 50n^2 - 40n + 1 \pmod{1000}, \\
19^n & \equiv 18n^2 + 1 \pmod{72}, \\
5^n & \equiv 96n^3 - 24n^2 - 68n + 1 \pmod{256}, \\
5^{2n} & \equiv 162n^5 + 540n^4 + 846n^3 + 288n^2 - 354n + 1 \pmod{1458}.
\end{align*}
\]

**References**


Stanley Rabinowitz  
12 Vine Brook Road  
Westford  
MA 01886 USA  
stan@MathProPress.com