Hindawi Publishing Corporation
Abstract and Applied Analysis
Volume 2014, Article ID 575064, 9 pages
http://dx.doi.org/10.1155/2014/575064

Research Article

Recursive Elucidation of Polynomial Congruences Using Root-Finding Numerical Techniques

M. Khalid Mahmood[1] and Farooq Ahmad[2]

[1] *Department of Mathematics, University of the Punjab, Lahore 54590, Pakistan*
[2] *Faculty of Information Technology, University of Central Punjab, Lahore 54500, Pakistan*

Correspondence should be addressed to M. Khalid Mahmood; khalid.math@pu.edu.pk

Received 5 March 2014; Revised 6 April 2014; Accepted 10 April 2014; Published 5 May 2014

Academic Editor: Sher Afzal Khan

In this paper we put forward a family of algorithms for lifting solutions of a polynomial congruence mod p to polynomial congruence mod p^k. For this purpose, root-finding iterative methods are employed for solving polynomial congruences of the form $ax^n \equiv b(\mathrm{mod}\ p^k)$, $k \geq 1$, where a, b, and $n > 0$ are integers which are not divisible by an odd prime p. It is shown that the algorithms suggested in this paper drastically reduce the complexity for such computations to a logarithmic scale. The efficacy of the proposed technique for solving negative exponent equations of the form $ax^{-n} \equiv b(\mathrm{mod}\ p^k)$ has also been addressed.

1. Introduction and Preliminaries

The scope of congruence in number theory is of vital importance. The use of iterative methods for solving nonlinear equations has become a valuable device for numerical analysts. This research work addresses some iterative methods for solving polynomial congruences of the form $ax^n \equiv b(\mathrm{mod}\ p^k), k \geq 1$ where a, b, and $n > 0$ are integers which are not divisible by an odd prime p. The root-finding recursive techniques have been discussed in [1–4] to get the inverse of numbers modulo prime powers, which is the motivation of the proposed research work. In this piece of work, we use higher order iterative methods with a particular focus on Householder's and Basic Family of Iteration Functions (for detail, see [5–7]) in order to find solutions of polynomial congruences of the form $ax^n \equiv b(\mathrm{mod}\ p^k), k \geq 1$.

Hensel's lemma is one of the most popular methods amongst the existing techniques for solving polynomial congruence modulo p^k. By applying Hensel's lemma on some polynomial congruence modulo p^k, it can be seen that the experience of the exposition of this lemma is strenuous and much more laborious. So the proposed technique endeavors to keep the elucidation consistently a little low to give advantage in finding the solution of such congruences by means of explicit iteration techniques which are quite fast in finding these solutions. The following are the two versions of well-known Hensel's lemma.

Theorem 1 (see [8]). *Suppose that $g(x)$ is a polynomial with integral coefficients. If $g(x) \equiv 0(\mathrm{mod}\ p^j)$ and $g'(a) \not\equiv 0(\mathrm{mod}\ p)$, then there is a unique $y(\mathrm{mod}\ p)$ such that $g(a + yp^j) \equiv 0(\mathrm{mod}\ p^{j+1})$.*

The following theorem can easily be deduced from Hensel's lemma after applying Taylor's Theorem. This is actually the typical procedure to find solutions of congruences modulo p^k by means of Hensel's lemma. For details see [9, page 106].

Theorem 2 (see [9]). *Let p be a prime and k an arbitrary positive integer, and suppose that s is a solution of $f(x) \equiv 0(\mathrm{mod}\ p^k)$.*

(1) *If $p \nmid f'(s)$, then there is precisely one solution s_{k+1} of $f(x) \equiv 0(\mathrm{mod}\ p^{k+1})$ such that $x_{k+1} \equiv s(\mathrm{mod}\ p^k)$ is given by $s_{k+1} = s + tp^k$, where t is the unique solution of $f'(s)t \equiv (-f(s)/p^k)(\mathrm{mod}\ p)$.*

(2) *If* $p \mid f'(s)$ *and* $p^{k+1} \mid f(s)$, *then there are* p *solutions of* $f(x) \equiv 0 (\mathrm{mod}\ p^{k+1})$ *that are congruent to* $s (\mathrm{mod}\ p^k)$, *given by* $s + p^k j$, *for* $j = 0, 1, 2, \ldots, p-1$.

(3) *If* $p \mid f'(s)$ *and* $p^{k+1} \nmid f(s)$, *then there are no solutions of* $f(x) \equiv 0 (\mathrm{mod}\ p^{k+1})$ *that are congruent to* $s (\mathrm{mod}\ p^k)$.

Let us solve the congruence $2x^3 \equiv 5 (\mathrm{mod}\ 7^4)$ using Theorem 2. Let $f(x) = 2x^3 - 5$. First, we solve $f(x) \equiv 0 (\mathrm{mod}\ 7)$. By trial, it is easy to find that $x \equiv 3 (\mathrm{mod}\ 7)$ and $x \equiv 4 (\mathrm{mod}\ 7)$ are the solutions of the congruence $f(x) \equiv 0 (\mathrm{mod}\ 7)$. To perform iterations by Theorem 2, we proceed as under.

Take $s = s_1 = 3$; then $7 \nmid f'(3)$. By Theorem 2, there is a unique solution s_2 of $f(x) \equiv 0 (\mathrm{mod}\ 7^2)$. To find s_2, we find integer t from the congruence $f'(3)t \equiv (-f(3)/7) (\mathrm{mod}\ 7)$. This gives $54t \equiv (-49/7) (\mathrm{mod}\ 7)$ or $t \equiv 0 (\mathrm{mod}\ 7)$. Hence the unique solution $s_{k+1} = s + tp^k$ gives $s_2 = 3$. Therefore $s_2 = 3$ is the unique solution of $f(x) \equiv 0 (\mathrm{mod}\ 7^2)$.

Next we take $s_2 = 3$; then $f'(3)t \equiv (-f(3)/7^2) (\mathrm{mod}\ 7)$ becomes $54t \equiv (-49/49) (\mathrm{mod}\ 7)$. That is, $5t \equiv 6 (\mathrm{mod}\ 7)$ or $t \equiv 4 (\mathrm{mod}\ 7)$. Hence the unique solution $s_3 = s_2 + tp^k$ gives $s_3 = 3 + 4 * 7^2 = 199$. Therefore, $s_2 = 199$ is the unique solution of $f(x) \equiv 0 (\mathrm{mod}\ 7^3)$.

Finally we take $s_3 = 199$; then $f'(199) = 277606$ is not divisible by 7. Thus there is a unique solution s_4 of $f(x) \equiv 0 (\mathrm{mod}\ 7^4)$. To find s_4, we solve $f'(199)t \equiv (-f(199)/7^3) (\mathrm{mod}\ 7)$. This gives $5t \equiv 4 (\mathrm{mod}\ 7)$ or $t \equiv 5 (\mathrm{mod}\ 7)$. Then, $s_4 = 199 + 5 * 7^3 = 1914$. Hence, $s_4 = 1914$ is the solution of $2x^3 \equiv 5 (\mathrm{mod}\ 7^4)$.

From above example, it is noticed that several iterations are required in order to compute a solution to a congruence of higher powers of prime which is computationally intensive. Moreover at each step we need to calculate derivative of the function at current root. Hence we may hesitate in solving polynomial congruences with modulus of higher powers of primes using this lemma. Thus we need to find some explicit algorithms in which the needed derivatives are already incorporated with some $\log k$ steps. In the underlying paper we solve the polynomial congruence with higher modulo by means of algorithms developed using root-finding iterative methods. The p-adic proof of these algorithms has been derived using elementary number theory. Notations used in this paper are standard and we follow [1–3, 10, 11].

2. A Solution of Congruences Using Newton's Method

Newton's method is a well-known iterative procedure for finding the roots of an equation. It is the best tool in many ways for the solution of a nonlinear problem. Its simplicity and great speed always attract in attempting a nonlinear problem. Assume that an initial estimate x_0 is known for the desired root α of $f(x) = 0$. Then to perform iterations the formula for Newton's method is

$$x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)}, \quad k = 0, 1, 2 \ldots \tag{1}$$

Let us take $f(x) = b/x^n - a$. Then using (1), the explicit form for Newton's method is

$$nbx_{k+1} = (n+1)\, bx_k - ax_k^{n+1}. \tag{2}$$

Like real numbers, it can be proved that Newton's method is quadratically convergent. Now if x_k is the solution of $ax^n \equiv b (\mathrm{mod}\ p^k)$ then for some integer t, we have, $ax_k^n = b + tp^k$. Then by using (2), we obtain

$$\begin{aligned} ax_{k+1}^n &= \frac{\left(b + tp^k\right)}{(nb)^n}\left\{(n+1)\, b - b - tp^k\right\}^n \\ &= \frac{\left(b + tp^k\right)}{(nb)^n}\left(nb - tp^k\right)^n \\ &= \frac{\left(b + tp^k\right)}{(nb)^n} \\ &\quad \times \left\{(nb)^n - n(nb)^{n-1}tp^k + \text{terms involving } p^{2k}\right\} \\ &\equiv \frac{\left(b + tp^k\right)}{(nb)^n}\left\{(nb)^n - n(nb)^{n-1}tp^k\right\}\left(\mathrm{mod}\ p^{2k}\right) \\ &\equiv \frac{(nb)^n b}{(nb)^n}\left(\mathrm{mod}\ p^{2k}\right). \end{aligned} \tag{3}$$

Now, if $a, b, n \not\equiv 0 (\mathrm{mod}\ p)$ then $(p, bn) = 1$ and hence $(p^{2k}, (bn)^n) = 1$. Then by Cancellation law, (3) yields that x_{k+1} is the solution of the congruence $ax^n \equiv b (\mathrm{mod}\ p^{2k})$.

Let us solve the congruence $2x^3 \equiv 3 (\mathrm{mod}\ 5^{32})$. In order to solve a polynomial congruence of the form $ax^n \equiv b (\mathrm{mod}\ p^{2k}), k \geq 1$, we first see that it is sufficient to solve $ax^n \equiv b (\mathrm{mod}\ p)$ since every solution of $ax^n \equiv b (\mathrm{mod}\ p^{2k})$ is a solution of $ax^n \equiv b (\mathrm{mod}\ p)$. Once we do this, then we can apply (2) for finding the solutions of $ax^n \equiv b (\mathrm{mod}\ p^{2k})$ from the solutions of the congruence $ax^n \equiv b (\mathrm{mod}\ p^k)$. Therefore, we first solve the congruence $2x^3 \equiv 3 (\mathrm{mod}\ 5)$. By inspection we see that $x \equiv 4 (\mathrm{mod}\ 5)$ is the solution of the congruence $2x^3 \equiv 3 (\mathrm{mod}\ 5)$. Thus we choose $x_1 = 4$ as our initial guess. Then by (2), we have

$$\begin{aligned} 9x_2 &= 4.3.4 - 2(4)^4 = -464 \\ &\equiv -414\left(\mathrm{mod}\ 5^2\right). \end{aligned} \tag{4}$$

Hence,

$$\begin{aligned} x_2 &\equiv -46\,(\mathrm{mod}\ 25) \\ &\equiv 4\,(\mathrm{mod}\ 25). \end{aligned} \tag{5}$$

We repeat above process and find that $x_3 \equiv 504, x_4 \equiv 368004, x_5 \equiv 88003883629$ and $x_6 \equiv 1996563532039908180504$ are the solutions of the given congruence modulo $5^4, 5^8, 5^{16}$, and 5^{32}, respectively.

2.1. Order of Convergence. As far as the convergence of an iterative method of order m is concerned, it avows that the accurateness or precision to compute the current approximation x_j is only mj digits. This means that if we start with an r-digit integer x_k as the initial estimate in some modulo p^{α}, then x_{k+1} would be a new approximation in modulo $p^{m\alpha}$ containing rm-digits.

To ensure that the Newton's method is quadratically convergent, we show that x_{k+1} will not be a solution if we expand the binomial $(nb - tp^k)^n$ up to terms involving p^2. For this, we rewrite the step

$$\begin{aligned} ax_{k+1}^n &= \frac{\left(b+tp^k\right)}{(nb)^n}\left(nb-tp^k\right)^n \\ &= \frac{\left(b+tp^k\right)}{(nb)^n}\left\{(nb)^n - n(nb)^{n-1}tp^k + \frac{n(n-1)}{2}\right. \\ &\qquad \left.\times(nb)^{n-2}t^2p^2 + \text{terms involving } p^{3k}\right\} \\ &\equiv \frac{\left(b+tp^k\right)}{(nb)^n}\left\{(nb)^n - n(nb)^{n-1}tp^k\right. \\ &\qquad \left. + \frac{n(n-1)}{2}(nb)^{n-2}t^2p^2\left(\text{mod } p^{3k}\right)\right\} \\ &\equiv \frac{b(nb)^n - ((n+1)/2)(nb)^{n-1}t^2p^2}{(nb)^n}\left(\text{mod } p^{3k}\right) \\ &\not\equiv b\left(\text{mod } p^{3k}\right) \quad \text{as} \quad -\frac{n+1}{2}(nb)^{n-1}t^2p^2 \\ &\not\equiv 0\left(\text{mod } p^{3k}\right). \end{aligned} \tag{6}$$

3. Third Order Iterative Methods

The following are the third order iterative methods for which the explicit formulas for finding the roots of congruences are presented. The p-adic proofs of their convergence is given in the following two theorems.

3.1. A Variant of Newton's Method. Several variants of Newton's method have been given by many researchers to improve the order of convergence. For third-order convergence, the following three variants of Newton's methods have been studied earlier in [11, 12] to solve nonlinear equations, given as

$$x_{k+1} = x_k - \frac{f(x_k)}{f'\left(x_{k+1}^*\right)}, \quad k \geq 0, \tag{7}$$

$$\text{where } x_{k+1}^* = x_k - \frac{f(x_k)}{2f'(x_k)} \tag{8}$$

$$\begin{aligned} x_{k+1} &= x_k - \frac{f\left(x_{k+1}^*\right)}{f'(x_k)}, \quad k \geq 0, \\ &\text{where } x_{k+1}^* = x_k - \frac{f(x_k)}{f'(x_k)}, \end{aligned} \tag{9}$$

$$\begin{aligned} x_{k+1} &= x_k - \frac{2f(x_k)}{f'\left(x_{k+1}^*\right) + f'(x_k)}, \quad k \geq 0 \\ &\text{where } \quad x_{k+1}^* = x_k - \frac{f(x_k)}{f'(x_k)}. \end{aligned} \tag{10}$$

In the following theorem, we use (7) to find the solutions of congruences of the form $ax^n \equiv b(\text{mod } p^{3k})$, $k \geq 1$, from the solutions of the congruence $ax^n \equiv b(\text{mod } p^k)$.

Theorem 3. *Let a, b, and $n > 0$ be integers which are not divisible by an odd prime p. If x_k, $k \geq 1$ satisfies $ax^n \equiv b(\text{mod } p^k)$ then x_{k+1} satisfies the congruence $ax^n \equiv b(\text{mod } p^{3k})$, where*

$$x_{k+1} = x_k\left[1 + \frac{\left(b - ax_k^n\right)\left\{(2n+1)b - ax_k^n\right\}^{n+1}}{2^{n+1}(nb)^{n+1}}\right] \tag{11}$$

Proof. To prove this, let $f(x) = b/x^n - a$. By (8), we get, $x_{k+1}^* = x_k(((2n+1)b - ax_k^n)/nb)$. Then by (7), we obtain

$$x_{k+1} = x_k\left[1 + \frac{\left(b - ax_k^n\right)\left\{(2n+1)b - ax_k^n\right\}^{n+1}}{2^{n+1}(nb)^{n+1}}\right]. \tag{12}$$

If x_k is the solution of $ax^n \equiv b(\text{mod } p^k)$ then for some integer t, we have $ax_k^n = b + tp^k$. Putting in (12), we get

$$\begin{aligned} &nb(2nb)^n x_{k+1} \\ &\quad = x_k\left[nb(2nb)^n - tp^k\right. \\ &\qquad \times\left\{(2nb)^n - n(2nb)^{n-1}tp^k\right. \\ &\qquad \left. - \frac{n(n-1)}{2}(2nb)^{n-2}t^2p^{2k}\right. \\ &\qquad \left.\left. + \text{terms involving } p^{3k}\right\}\right] \\ &\quad \equiv x_k\left\{nb(2nb)^n - tp^k(2nb)^n\right. \\ &\qquad \left. + n(2nb)^{n-1}t^2p^{2k}\right\}\left(\text{mod } p^{3k}\right). \end{aligned} \tag{13}$$

Since $p > 2$ and $(2nb, p) = 1$, so $((2nb)^{n-1}, p^{3k})) = 1$. Then by (13)

$$2(nb)^2 x_{k+1} = x_k \left\{2(nb)^2 - 2nbtp^k + nt^2 p^{2k}\right\} \left(\mathrm{mod}\ p^{3k}\right). \tag{14}$$

This implies that

$$\begin{aligned} ax_{k+1}^n &\equiv \left(b + tp^k\right) \\ &\quad \times \frac{\left(2(nb)^2 - 2nbtp^k + nt^2 p^{2k}\right)^n}{\left(2\,(nb)^2\right)^n} \left(\mathrm{mod}\ p^{3k}\right) \\ &\equiv \frac{b\left(2\,(nb)^2\right)^n}{\left(2\,(nb)^2\right)^n} \left(\mathrm{mod}\ p^{3k}\right) \\ &\equiv b \left(\mathrm{mod}\ p^{3k}\right) \quad \text{as} \quad (2nb, p) = 1. \end{aligned} \tag{15}$$

□

3.2. Abbasbandy's Method. In [10], Abbasbandy used Adomian decomposition method to improve Newton's method for solving nonlinear equations. The improved method is called Abbasbandy's method (AM). Solving polynomial congruences is one of the most interesting problems in number theory. In this section, we use AM to solve polynomial congruences of the form $ax^n \equiv b(\mathrm{mod}\ p^k)$, $k \geq 1$. It can be seen that AM lifts a solution modulo p to p^3 then to p^9 and by iteration to p^{3^k}. To perform iterations, the formula for AM is expressed as

$$x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)} - \frac{f^2(x_k) f''(x_k)}{2f'^3(x_k)} - \frac{f^3(x_k) f'''(x_k)}{6f'^4(x_k)}. \tag{16}$$

Theorem 4. *Let a, b, and $n > 0$ be integers which are not divisible by a prime $p > 3$. If x_k, $k \geq 1$ satisfies $ax^n \equiv b(\mathrm{mod}\ p^k)$ then x_{k+1} satisfies the congruence $ax^n \equiv b(\mathrm{mod}\ p^{3k})$, where*

$$\begin{aligned} 6n^3b^3 x_{k+1} &= x_k \left(2b^3 \left(1 + 3n + 5n^2 + 3n^3\right)\right. \\ &\quad - 3ab^2 \left(2 + 5n + 5n^2\right) x_k^n \\ &\quad + 6a^2 b(1+n)^2 x_k^{2n} \\ &\quad \left. - a^3 \left(2 + 3n + n^2\right) x_k^{3n}\right). \end{aligned} \tag{17}$$

Proof. To prove this, let $f(x) = b/x^n - a$. By (16), we obtain

$$\begin{aligned} x_{k+1} &= x_k - \frac{b/x_k^n - a}{-nb/x_k^{n+1}} - \frac{\left(b/x_k^n - a\right)^2 \left(n\,(n+1)\,b/x_k^{n+2}\right)}{2\left(-nb/x_k^{n+1}\right)^3} \\ &\quad + \frac{\left(b/x_k^n - a\right)^3 \left(\left(n\,(n+1)\,(n+2)\,b\right)/x_k^{n+3}\right)}{6\left(-nb/x_k^{n+1}\right)^4} \\ &= x_k \left[1 + \frac{b - ax_k^n}{nb} + \frac{\left(b - ax_k^n\right)^2 (n+1)}{2n^2b^2} \right. \\ &\quad \left. + \frac{\left(b - ax_k^n\right)^3 (n+1)\,(n+2)}{6n^3b^3}\right]. \end{aligned} \tag{18}$$

This can be simplified as

$$\begin{aligned} &6n^3b^3 x_{k+1} \\ &= x_k \left[6b^3n^3 + \left(b - ax_k^n\right) 6n^2b^2 \right. \\ &\quad + \left(b - ax_k^n\right)^2 (n+1)\, 3nb \\ &\quad \left. + \left(b - ax_k^n\right)^3 (n+1)\,(n+2)\right] \\ &= x_k \left(2b^3 \left(1 + 3n + 5n^2 + 3n^3\right)\right. \\ &\quad - 3ab^2 \left(2 + 5n + 5n^2\right) x_k^n \\ &\quad \left. + 6a^2b(1+n)^2 x_k^{2n} - a^3 \left(2 + 3n + n^2\right) x_k^{3n}\right). \end{aligned} \tag{19}$$

Next we show that x_{k+1} is a solution of the congruence $ax^n \equiv b(\mathrm{mod}\ p^{3k})$. Now if x_k is the solution of $ax^n \equiv b(\mathrm{mod}\ p^k)$ then for some integer t, we have, $ax_k^n = b + tp^k$. Putting in (19), we get

$$\begin{aligned} &6n^3b^3 x_{k+1} \\ &= x_k \left[2b^3 \left(1 + 3n + 5n^2 + 3n^3\right)\right. \\ &\quad - 3b^2 \left(2 + 5n + 5n^2\right) \left(b + tp^k\right) \\ &\quad + 6b(1+n)^2 \left(b^2 + 2btp^k + t^t p^{2k}\right) \\ &\quad - \left(2 + 3n + n^2\right) \left(b^3 + 3b^2 tp^k\right. \\ &\qquad \left.\left. + 3bt^2 p_{2k} + t^3 p^{3k}\right)\right] \\ &\equiv x_k \left[6n^3b^3 - 6n^2b^2 tp^k\right. \\ &\quad \left. + 3n\,(n+1)\, bt^2 p^{2k}\right] \left(\mathrm{mod}\ p^{3k}\right). \end{aligned} \tag{20}$$

This implies that

$$\begin{aligned} &\left(6n^3b^3\right)^n ax_{k+1}^n \\ &\equiv \left[6n^3b^3 - 6n^2b^2 tp^k + 3n\,(n+1)\, bt^2 p^{2k}\right]^n \left(\mathrm{mod}\ p^{3k}\right). \end{aligned} \tag{21}$$

Using Binomial Series expansion, we obtain

$$\begin{aligned} &\left(6n^3b^3\right)^n ax_{k+1}^n \\ &\equiv \left[\left(6n^3b^3\right)^n + n\left(6n^3b^3\right)^{n-1}\right. \end{aligned}$$

$$\times \left(-6n^2b^2tp^k + 3n(n+1)bt^2p^{3k}\right) + \frac{n(n-1)}{2}\left(6n^3b^3\right)^{n-2} \times \left(-6n^2b^2tp^k + 3n(n+1)bt^2p^{2k}\right)^2 + \text{terms involving } p^{3k}\Big]\left(b+tp^k\right)\left(\text{mod } p^{3k}\right)$$
$$\equiv \Big[\left(6n^3b^3\right)^n - 6n^3b^2\left(6n^3b^3\right)^{n-1}tp^k + 6n^3b\left(6n^3b^3\right)^{n-1}t^2p^{2k}\Big]\left(b+tp^k\right)\left(\text{mod } p^{3k}\right)$$
$$\equiv b\left(6n^3b^3\right)^n\left(\text{mod } p^{3k}\right). \tag{22}$$

Since $p > 3$ and $(nb, p) = 1$, so $(6n^3b^3, p) = 1$ and hence $((6n^3b^3)^n, p^{3k}) = 1$. Finally, by Cancelation law (22) yields that x_{k+1} is the solution of the congruence $ax^2 \equiv b(\text{mod } p^{3k})$. □

3.3. Remark. Note that variants of Newton's method discussed in Section 3 are the two-step (predictor-corrector) methods while the followings are one-step methods. This clearly shows that the technique suggested is equally good even to two step methods and could be enhanced to multistep methods.

4. Higher Order Iterative Families

The following are the two well-known one step root-finding higher order iterative families. In this section, we make use of these families in order to find the solutions of congruences modulo p^k. The following theorems demonstrate how one can employ the order of convergence of these families to get the solutions of ecstatic problems in number theory.

4.1. Householder's Family. Householder's methods are a class of well-known iterative algorithms for solving a nonlinear equation in one variable. Let f be a function of one variable with continuous derivatives of order $p+1$. The formula for Householder's method of order $p+1$ to perform iterations is

$$x_{k+1} = x_k + p\frac{(1/f)^{p-1}(x_k)}{(1/f)^p(x_k)}. \tag{23}$$

Let us establish a formula for $p = 3$ using (23)

$(p-1)$th derivative of $1/f(x)$

$$= \frac{2f'(x)^2}{f(x)^3} - \frac{f''(x)}{f(x)^2}. \tag{24}$$

Similarly, pth derivative of $1/f(x)$

$$= -\frac{6f'(x)^3}{f(x)^4} + \frac{6f'(x)f''(x)}{f(x)^3} - \frac{f'''(x)}{f(x)^2}. \tag{25}$$

Substituting the values of (24) and (25) into (23), we obtain

$$x_{k+1} = \Big(3f(x_k)\left[f(x_k)f''(x_k) - 2f'(x_k)^2\right] \times \left(f(x_k)^2f'''(x_k) + 6f'(x_k)^3 - 6f(x_k)f'(x_k)f''(x_k)\right)^{-1}\Big) + x_k. \tag{26}$$

In the following theorem, we use Householder's method of order 4 in order to find the solutions of congruences of the form $ax^n \equiv b(\text{mod } p^{4k})$, $k \geq 1$, from the solutions of the congruence $ax^n \equiv b(\text{mod } p^k)$.

Theorem 5. *Let a, b, and $n > 0$ be integers which are not divisible by a prime $p > 3$. If x_k, $k \geq 1$ is a solution of the congruence $ax^n \equiv b(\text{mod } p^k)$ then x_{k+1} is the solution of the congruence $ax^n \equiv b(\text{mod } p^{4k})$ satisfying the equation*

$$x_{k+1} = \Big(\left(b^2\left(n^2-1\right) + 2ab\left(2n^2+1\right)x_k^n + a^2\left(n^2-1\right)x_k^{2n}\right) \times \left(b^2(n-1)(n-2) + 4ab\left(n^2-1\right)x_k^n + a^2(n+1)(n+2)x_k^{2n}\right)^{-1}\Big)x_k. \tag{27}$$

Proof. To prove this, let $f(x) = b/x^n - a$ and solve $f(x) = 0$ using (26); we get

$$x_{k+1} = \left(3\left(\frac{b}{x_k^n} - a\right)\left[\left(\frac{b}{x_k^n} - a\right)\left(\frac{n(n+1)b}{x_k^{n+2}}\right) - 2\frac{n^2b^2}{x_k^{2n+2}}\right] \times \left(\left(\frac{b}{x_k^n} - a\right)^2\left(-\frac{n(n+1)(n+2)b}{x_k^{n+3}}\right) - 6\frac{n^3b^3}{x_k^{3n+3}} + 6\frac{n^2(n+1)b^2}{x_k^{2n+3}}\left(\frac{b}{x_k^n} - a\right)\right)^{-1}\right) + x_k$$
$$= \Big(3x_k\left(b - ax_k^n\right)\left[n(n+1)\left(b - ax_k^n\right) - 2n^2b^2\right] \times \left(6n^2(n+1)b^2\left(b - ax_k^n\right) - \left(b - ax_k^n\right)n \times (n+1)(n+2)bx_k^n - 6n^3b^3\right)^{-1}\Big) + x_k$$
$$= \Big(\left(b^2\left(n^2-1\right) + 2ab\left(2n^2+1\right)x_k^n + a^2\left(n^2-1\right)x_k^{2n}\right) \times \left(b^2(n-1)(n-2) + 4ab\left(n^2-1\right)x_k^n + a^2(n+1)(n+2)x_k^{2n}\right)^{-1}\Big)x_k. \tag{28}$$

Next we show that x_{k+1} is a root of the congruence $ax^n \equiv b(\mathrm{mod}\ p^{4k})$. Now if x_k is the solution of $ax^n \equiv b(\mathrm{mod}\ p^k)$ then for some integer t, we have, $ax_k^n = b + tp^k$. Putting in (27), we obtain

$$\begin{aligned} x_{k+1} = &\left(\left(b^2\left(n^2-1\right)+2b\left(2n^2+1\right)\left(b+tp^k\right)\right.\right.\\ &\left.+\left(n^2-1\right)\left(b+tp^k\right)^2\right)\\ &\times\left(b^2(n-1)(n-2)+4b\left(n^2-1\right)\left(b+tp^k\right)\right.\\ &\left.\left.+(n+1)(n+2)\left(b+tp^k\right)^2\right)^{-1}\right)x_k \qquad (29)\\ = &\left(\left(6n^2b^2+6n^2btp^k+\left(n^2-1\right)t^2p^{2k}\right)\right.\\ &\times\left(6n^2b^2+6n(n+1)btp^k\right.\\ &\left.\left.+(n+1)(n+2)t^2p^{2k}\right)^{-1}\right)x_k. \end{aligned}$$

This implies that

$$\begin{aligned} ax_{k+1}^n \equiv &\left(\left(b\left\{6n^2b^2+6n^2btp^k+\left(n^2-1\right)t^2p^{2k}\right\}^n\right)\right.\\ &\times\left(b\left\{6n^2b^2+6n(n+1)btp^k\right.\right.\\ &\left.\left.\left.+(n+1)(n+2)t^2p^{2k}\right\}^n\right)^{-1}\right)\left(b+tp^k\right). \end{aligned} \qquad (30)$$

Using Binomial Series expansion, we obtain

$$\begin{aligned} &\left[6n^2b^2+6n^2btp^k+\left(n^2-1\right)t^2p^{2k}\right]^n\left(b+tp^k\right)\\ &\quad=6^n(nb)^{2n}b+6^n n(nb)^{2n}tp^k\\ &\qquad+6^{n-1}(n-1)\left(3n^2+n+1\right)(nb)^{2n-1}t^2p^{2k}\\ &\qquad+6^{n-1}n(n-1)\left(n^3-n^2-1\right)(nb)^{2n-2}t^3p^{3k}\\ &\qquad+6^n(nb)^{2n}tp^k+6n^26^{n-1}(nb)^{2n-1}t^2p^{2k}\\ &\qquad+6^{n-1}n(n-1)\left(3n^2+n+1\right)(nb)^{2n-2}t^3p^{3k}\\ &\qquad+\text{terms involving } p^{4k}\\ &\quad\equiv 6^n(nb)^{2n}b+6^n(n+1)(nb)^{2n}tp^k\\ &\qquad+6^{n-1}\left(3n^3+4n^2-1\right)(nb)^{2n-1}t^2p^{2k}\\ &\qquad+6^{n-1}n^2(n-1)(n+1)^2(nb)^{2n-2}t^3p^{3k}\left(\mathrm{mod}\ p^{4k}\right). \end{aligned} \qquad (31)$$

Similarly, we expand denominator to get

$$\begin{aligned} &b\left[6n^2b^2+6n(n+1)btp^k\right.\\ &\qquad\left.+(n+1)(n+2)t^2p^{2k}\right]^n\\ &\quad=6^n(nb)^{2n}b+6^n(n+1)(nb)^{2n}tp^k\\ &\qquad+6^{n-1}(n+1)(n+2)(nb)^{2n-1}t^2p^{2k}\\ &\qquad+6^{n-1}(n+1)^2(n-1)(n+2)(nb)^{2n-2}t^3p^{3k}\\ &\qquad+3.6^{n-1}(n-1)(n+1)^2(nb)^{2n-1}t^2p^{2k}\\ &\qquad+6^{n-1}(n-1)(n+1)^3(n-2)(nb)^{2n-2}t^3p^{3k}\\ &\qquad+\text{terms involving } p^{4k}\\ &\quad\equiv 6^n(nb)^{2n}b+6^n(n+1)(nb)^{2n}tp^k\\ &\qquad+6^{n-1}\left(3n^3+4n^2-1\right)(nb)^{2n-1}t^2p^{2k}\\ &\qquad+6^{n-1}n^2(n-1)(n+1)^2(nb)^{2n-2}t^3p^{3k}\left(\mathrm{mod}\ p^{4k}\right). \end{aligned} \qquad (32)$$

Substituting (31) and (32) into (30), we get

$$\begin{aligned} ax_{k+1}^n \equiv &\frac{bd}{d}\left(\mathrm{mod}\ p^{4k}\right)\text{ where,}\\ d = &6^n(nb)^{2n}b+6^n(n+1)(nb)^{2n}tp^k\\ &+6^{n-1}\left(3n^3+4n^2-1\right)(nb)^{2n-1}t^2p^{2k}\\ &+6^{n-1}n^2(n-1)(n+1)^2(nb)^{2n-2}t^3p^{3k}. \end{aligned} \qquad (33)$$

Next we claim that $d \not\equiv 0\ (\mathrm{mod}\ p)$. To prove our assertion we let $d = 6^n(nb)^{2n}b + 6^n(n+1)(nb)^{2n}tp^k + 6^{n-1}(3n^3 + 4n^2 - 1)(nb)^{2n-1}t^2p^{2k} + 6^{n-1}n^2(n-1)(n+1)^2(nb)^{2n-2}t^3p^{3k} \equiv 0(\mathrm{mod}\ p)$. But then $6^n(nb)^{2n}b \equiv 0(\mathrm{mod}\ p)$. This shows that $(nb)^{2n} \equiv 0(\mathrm{mod}\ p)$ as $p > 3$ and $(b, p) = 1$. Which further implies that $p \mid nb$, a contradiction since $(nb, p) = 1$. Hence we conclude that $d \not\equiv 0(\mathrm{mod}\ p)$ and so because $d \not\equiv 0(\mathrm{mod}\ p^{4k})$. Thus by (33), x_{k+1} is the solution of the congruence $ax^2 \equiv b(\mathrm{mod}\ p^{4k})$. □

4.2. Basic Family of Iteration Functions. Basic family of iteration functions denoted by $B_m(x)$ is a well-known class of iterative algorithms of order m for solving a nonlinear equation in one variable. The details of Basic Family and its mathematical interpretation regarding existence and characterizations have been discoursed earlier in [5]. It has been proved that the members of this family like B_2 and B_3 coincide with well-known Newton's and Halley's methods. We further see that the member $B_4(x)$ coincides with a member of Householder's Family of order four. However, we demonstrate that the Basic family of iteration functions is more convenient in finding roots of the given congruence with desired convergence. To find the solutions of congruences

modulo p^k, we need to recall the basics of this family as given in [5] (for details see pages 1–3 in [5]).

Let $f(x)$ be a polynomial of degree ≥ 2 over the field of complex numbers. For integer $m \geq 2$, let $L_m(x)$ be a square matrix of order m whose diagonals elements are $f(x)$ defined as

$$L_m(x) = \begin{pmatrix} f(x) & 0 & 0 & \cdots & 0 \\ f'(x) & f(x) & 0 & \cdots & 0 \\ \frac{f''(x)}{2} & f'(x) & f(x) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{f^{m-1}(x)}{(m-1)!} & \frac{f^{m-2}(x)}{(m-2)!} & \frac{f^{m-3}(x)}{(m-3)!} & \cdots & f(x) \end{pmatrix}. \tag{34}$$

For $j = 12, \ldots$, let $L_m^j(x)$ be a square matrix of order $m - j$ obtained by removing first j rows and last j columns of the matrix $L_m(x)$ together with $L_1^1(x) = 1$ given as

$$L_m^j(x) = \begin{pmatrix} \frac{f^j(x)}{j!} & \frac{f^{j-1}(x)}{(j-1)!} & \cdots & 0 \\ \frac{f^{j+1}(x)}{(j+1)!} & \frac{f^j(x)}{j!} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \frac{f^{m-1}(x)}{(m-1)!} & \frac{f^{m-2}(x)}{(m-2)!} & \cdots & \frac{f^j(x)}{j!} \end{pmatrix}. \tag{35}$$

The family of iteration functions $B_m(x)$ is termed as Basic Family of iteration function of order m, where

$$B_m(x) = x - f(x) \frac{\det\left(L_{m-1}^1(x)\right)}{\det\left(L_m^1(x)\right)}. \tag{36}$$

Let us establish a formula for $m = 4$. Then by (36), we obtain

$$B_4(x) = x - f(x) \frac{\det\left(L_3^1(x)\right)}{\det\left(L_4^1(x)\right)} \tag{37}$$

Now

$$L_4^1(x) = \begin{pmatrix} f'(x) & f(x) & 0 \\ \frac{f''(x)}{2!} & f'(x) & f(x) \\ \frac{f'''(x)}{3!} & \frac{f''(x)}{2!} & f'(x) \end{pmatrix}. \tag{38}$$

Then

$$\det\left(L_4^1(x)\right) = \left(f'(x)\right)^3 - \frac{1}{2} f(x) f'(x) f''(x) + \frac{1}{6}\left(f(x)\right)^2 f'''(x). \tag{39}$$

Similarly,

$$L_3^1(x) = \begin{pmatrix} f'(x) & f(x) \\ \frac{f''(x)}{2!} & f'(x) \end{pmatrix}. \tag{40}$$

Then

$$\det\left(L_3^1(x)\right) = \left(f'(x)\right)^2 - \frac{1}{2} f(x) f''(x). \tag{41}$$

Substituting (39) and (41) into (37), after simplifying we obtain

$$B_4(x) = x - \frac{6 f(x)\left(f'(x)\right)^2 - 3\left(f(x)\right)^2 f''(x)}{\left(f(x)\right)^2 f'''(x) + 6\left(f'(x)\right)^3 - 6 f(x) f'(x) f''(x)}. \tag{42}$$

Now by (26) and (42), it is interesting to notice that both families are mapped onto each other even for fourth order members. That is, the iteration function of Householder's family for $d = 3$ and the iteration function B_4 for Basic Family are same. Therefore, the fourth order convergence for p-adic analysis of Basic Family as proved in Theorem 5 is instinctively established. However, the Basic Family is certainly more expedient to find solutions of congruences modulo p^k as one can find the desired solution using (36) as well. Let us again find the solution of $2x^3 \equiv 5 \pmod{7^4}$ through determinants. Here $f(x) = 5/x^3 - 3$ and $x = 3$ is the initial solution. Then by (37),

$$\det\left(L_4^1(3)\right) = \det\begin{pmatrix} \frac{-5}{27} & \frac{-49}{27} & 0 \\ \frac{10}{81} & \frac{-5}{27} & \frac{-49}{27} \\ \frac{-50}{729} & \frac{10}{81} & \frac{-5}{27} \end{pmatrix} \equiv 923 \pmod{7^4}. \tag{43}$$

Similarly,

$$\det\left(L_3^1(3)\right) = \det\begin{pmatrix} \frac{-5}{27} & \frac{-49}{27} \\ \frac{10}{81} & \frac{-5}{27} \end{pmatrix} \equiv 592 \pmod{7^4}. \tag{44}$$

Substituting the values into (37), we obtain

$$\begin{aligned} x_{k+1} = B_4(x) &\equiv 3 + \frac{49(592)}{27(923)} \pmod{7^4} \\ &\equiv \frac{528}{904} \pmod{7^4} \\ &\equiv 1914 \pmod{7^4}. \end{aligned} \tag{45}$$

4.3. Remarks

(1) The overhead methods also give an equally efficient technique in solving polynomial congruences modulo p^k with negative-exponent. To find the solutions of the congruence $az^{-n} \equiv b(\mathrm{mod}\ p^k)$, we solve the congruence $ay^n \equiv b(\mathrm{mod}\ p^k)$, where $zy \equiv 1(\mathrm{mod}\ p^k)$. This means that the solution of the first congruence is the multiplicative inverse of the solution of the later congruence. We claim that the linear congruence $\alpha z \equiv 1(\mathrm{mod}\ p^k)$ is always solvable, where α is the solution of the congruence $ay^n \equiv b(\mathrm{mod}\ p^k)$. Then α must be a solution of the congruence $ay^n \equiv b(\mathrm{mod}\ p)$. That is $a\alpha^n \equiv b(\mathrm{mod}\ p)$. Since $p \nmid b$, so $p \nmid a\alpha^n$. This clearly shows that $p \nmid \alpha$. Hence $(\alpha, p) = 1$. Consequently, the linear congruence $\alpha z \equiv 1(\mathrm{mod}\ p^k)$ is solvable as we know that the linear congruence $\alpha z \equiv 1(\mathrm{mod}\ p^k)$ is solvable if and only if $(\alpha, p) = 1$. Let β be the solution of the linear congruence $\alpha z \equiv 1(\mathrm{mod}\ p^k)$. Then β is the desired solution of $az^{-n} \equiv b\,(\mathrm{mod}\ p^k)$. By (45), $y \equiv 1914(\mathrm{mod}\ 7^4)$ satisfies $2y^3 \equiv 5(\mathrm{mod}\ 7^4)$. To find a solution of $2z^{-3} \equiv 5(\mathrm{mod}\ 7^4)$, we solve the linear congruence $1914z \equiv 1(\mathrm{mod}\ 7^4)$. It is easy to see that $z = \beta \equiv 2189(\mathrm{mod}\ 7^4)$ is its solution. Hence, $\beta \equiv 2189(\mathrm{mod}\ 7^4)$ is the desired solution of the congruence $2z^{-3} \equiv 5\ (\mathrm{mod}\ 7^4)$.

(2) The text does not discuss the well-known Halley's third order iterative method as it can be seen that it is a subcase of both families discussed above. In the Householder's family for $d = 2$ and in basic iteration family for $m = 3$, the results yield Halley's method.

In the following algorithm, we summarize the solutions of congruences discussed in Theorems 3, 4, and 5.

4.4. Algorithm. Step 1: Set x_1 as initial estimate.

Step 2:

$$k = \begin{cases} \log_3 m, & \text{if Equation (10) or (16) is used.} \\ \log_4 m, & \text{if Equation (26) is used.} \end{cases} \tag{46}$$

Step 3: For $i = 1$ to k do

$$x_{i+1} = \begin{cases} f(x_i) \bmod p^{3m}, & \text{if Equation (10) or (16) is used.} \\ f(x_i) \bmod p^{4m}, & \text{if Equation (26) is used.} \end{cases} \tag{47}$$

Step 4: Solution = x_{i+1}

The following algorithm is an improved form of the above given algorithms for any arbitrary value of q where q is the order of convergence of the iterative method induced.

Step 1: Set x_1 as initial estimate.

Step 2:

$$k = \log_q m, \qquad q = 3, 4, \ldots \tag{48}$$

Step 3: For $i = 1$ to k do

$$x_{i+1} = f(x_i) \bmod p^{qm} \tag{49}$$

Step 4: Solution = x_{i+1}

5. Numerical Examples

Let us solve the congruence $2x^3 \equiv 5(\mathrm{mod}\ 7^{81})$ by using Hensel's lemma (HL), Abbasbandy's method (AM), a variant of Newton's method (VN), Householder's method (HM), and Basic Family's (BM) method. In order to solve a polynomial congruence of the form $ax^n \equiv b(\mathrm{mod}\ p^k), k \geq 1$, it is sufficient to solve $ax^n \equiv b(\mathrm{mod}\ p)$. Once we do this, then we can apply algorithm given Section 4.4 for finding the solutions of $ax^n \equiv b\,(\mathrm{mod}\ p^{3k})$ from the solutions of the congruence $ax^n \equiv b(\mathrm{mod}\ p^k)$. Therefore, we first solve the congruence $2x^3 \equiv 5(\mathrm{mod}\ 7)$. By inspection we see that $x \equiv 3(\mathrm{mod}\ 7)$ and $x \equiv 4(\mathrm{mod}\ 7)$ are the solutions of the congruence $2x^3 \equiv 5(\mathrm{mod}\ 7)$. Thus we choose $x_1 = 3$ as our initial guess. Then by Algorithm given in Section 4.4, we have

$$x_2 \equiv 3\left(\mathrm{mod}\ 7^2\right), \qquad x_2 \equiv 199\left(\mathrm{mod}\ 7^3\right). \tag{50}$$

We repeat above process to find the roots of the given congruence modulo 7^4, 7^8,7^9 and so on until we get the solution of the congruence $2x^3 \equiv 5(\mathrm{mod}\, 7^{81})$. The necessary computations are summarized in Table 1.

6. Conclusion

The complexity of a typical method for numerical computations using Theorem 2 is linear. In the underlying work we have suggested various methods that drastically reduce the complexity for such computations to a logarithmic scale. It is easily deduced from the algorithm given in Section 4.4 that the complexity of the described method is $O(\log m)$. Additionally the method developed is an explicit technique which does not require any numerical computation for finding any sort of derivative. Therefore, the techniques developed in this paper perform much faster for values of m in powers of $3, 4, \ldots$ in contrast with existing techniques for solving polynomial congruences. Moreover the research work proves that both families of iterative function, that is, the Householder's and Basic iteration family work p-adically as shown in various results. Furthermore we have shown the efficacy of the given method for solving negative exponent equations of the form $ax^{-n} \equiv b$.

Table 1: Comparison of HL, AM/VN, and HM/BM.

Methods	$x_k \pmod{p^{\alpha}}$	$x_{k+1} \pmod{p^{m\alpha}}$
HL	3	$3 \pmod{7^2}$
AM/VN	3	$199 \pmod{7^3}$
HM/BM	3	$1914 \pmod{7^4}$
HL	3	$199 \pmod{7^3}$
AM/VN	199	$37399890 \pmod{7^9}$
HM/BM	1914	$24211798063820 \pmod{7^{16}}$
HL	199	$1914 \pmod{7^4}$
AM/VN	37399890	$43741341794232381830191 \pmod{7^{27}}$
HM/BM	24211798063820	$954381941076\ldots900159613690770 \pmod{7^{64}}$
HL	1914	$573 \pmod{7^5}$
AM/VN	43741341794232381830191	$24452773833\ldots232537600 \pmod{7^{81}}$

Solution of the congruence $2x^3 \equiv 5 \pmod{7^{81}}$ with initial estimate $x_1 = 3$.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] E. V. Krishnamurthy and V. K. Murthy, "Fast iterative division of p-adic numbers," *IEEE Transactions on Computers*, vol. 32, no. 4, pp. 396–398, 1983.

[2] E. V. Krishnamurthy, "On optimal iterative schemes for high-speed division," *IEEE Transactions on Computers*, vol. 20, pp. 227–231, 1970.

[3] M. P. Knapp and C. Xenophontos, "Numerical analysis meets number theory: using rootfinding methods to calculate inverses mod p^n," *Applicable Analysis and Discrete Mathematics*, vol. 4, no. 1, pp. 23–31, 2010.

[4] E. Bach, "Iterative root approximation in p-adic numerical analysis," *Journal of Complexity*, vol. 25, no. 6, pp. 511–529, 2009.

[5] B. Kalantari, I. Kalantari, and R. Zaare-Nahandi, "A basic family of iteration functions for polynomial root finding and its characterizations," *Journal of Computational and Applied Mathematics*, vol. 80, no. 2, pp. 209–226, 1997.

[6] A. S. Householder, *The Numerical Treatment of a Single Nonlinear Equation*, McGraw-Hill, 1970.

[7] J. M. Ortega and W. C. Rheinboldt, *Iterative Solution of Nonlinear Equations in Several Variables*, Academic Press, 1970.

[8] I. Nivan and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley & Sons, 2005.

[9] A. Adler and J. E. Coury, *The Theory of Numbers*, Jones and Bartlett Publishers, Boston, Mass, USA, 1995.

[10] S. Abbasbandy, "Improving Newton-Raphson method for nonlinear equations by modified Adomian decomposition method," *Applied Mathematics and Computation*, vol. 145, no. 2-3, pp. 887–893, 2003.

[11] S. Weerakoon and T. G. I. Fernando, "A variant of Newton's method with accelerated third-order convergence," *Applied Mathematics Letters*, vol. 13, no. 8, pp. 87–93, 2000.

[12] A. Y. Özban, "Some new variants of Newton's method," *Applied Mathematics Letters*, vol. 17, no. 6, pp. 677–682, 2004.

[13] J. F. Traub, *Iterative Methods for Solutions of Equations*, Prentice-Hall, Englewood Cliffs, NJ, USA, 1964.