A NOVEL TECHNIQUE FOR THE ELUCIDATION OF LINEAR AND QUADRATIC CONGRUENCES

M. K.Mahmood and Y. D. Khan*

Department of Mathematics, University of the Punjab, Lahore
*Faculty of Information Technology, University of Management and Technology, Lahore Corresponding Author E-mail Address: khalid.math@pu.edu.pk

ABSTRACT: Explicit iteration formulas were proposed for solving the equation $f(x) \equiv 0 \bmod p^k$, when f was the polynomial $ax^n - b$. Speedy algorithms were formulated for lifting solutions of a polynomial congruence mod p, to polynomial congruence mod p^k. This was done reasonably fast, using proposed algorithm. Polynomial time was ***k***, which was about the best possible since the number of bits in the answer was in general proportional to ***k***. The algorithm developed was instigated with an adaptation of secant method. For a polynomial ***f***, with initial solutions $x_0 \bmod p^{k_1}$ and $x_1 \bmod p^{k_2}$ to $f(x) \equiv 0 \bmod p^k$, haggled a solution x_2 to $f(x) \equiv 0 \bmod p^{k_1+k_2}$ with, $x_2 = x_1 - \frac{f(x_1)(x_1 - x_0)}{f(x_1) - f(x_0)}$, where the inverse was computed using the Euclidean algorithm in the ring of integers modulo p^k. The proposed technique endeavored to keep the elucidation consistently a little low to give advantage in finding the solution of congruences by means of explicit iteration techniques which proved quite fast in finding these solutions.

Key words: Congruences, Secant method, Euclidean algorithm, Polynomial modulo p^k, Integers modulo p^k.

(Received 02-01-2015 Accepted 30-07-2015)

INTRODUCTION

In the past researchers have given numerical methods to solve congruences using prime divisors. The study of (Krishnamurthy and Murthy, 1983) describes a fast iterative scheme based on the Newton's method for finding the reciprocal of finite segment p-adic numbers. The work of (Andersen and Jenkins, 2013) shows that the problem of division is reducible to the classical problem of finding the zeros of a polynomial. Hence, making it possible to use an algorithm which find zeros in a polynomial for division. The work of (Eric, 2009) elaborates several tricks for *p*-adic numerical analysis. An idea to reduce every polynomial to either linear or quadratic congruence is proposed by (Eugen, 2006). Several forms of Newton's iterative methods are discussed by (Stoer and Bulirsch, 2013 and Ben, 1997). Also, the research work of (Michal and Xenophontos 2010) explains that iterative methods are useful for calculating the inverse of numbers modulo prime powers. The concept of finding inverse modulo prime powers is significant for understanding the solution of a linear congruence of the form $ax \equiv 1 (mod\ p^k)$. Thus it becomes interesting to find solutions of congruences of the type $ax^n \equiv b\,(\text{mod } p^k), k \geq 1$ through Numerical Analysis as this is the generalization of the above case in a sense that if $n = 1$ and $b = 1$ is substituted in last equation then all of the results for finding the inverse of numbers modulo prime powers are produced. The typical procedure for solving polynomial congruences is the well-known Hensel lemma. Also, while solving an arbitrary polynomial congruence modulo with higher power of primes, it is observed that the application of the lemma is difficult and arduous. The following is the well-known version of Hensel's Lemma reported by (Ivan and Zuckerman, 2005) and (Thomas, 2005). Some other manipulations of this lemma are found by (Adler and Coury, 1995) and (David, 2007).

Hensel's Lemma: Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(x) \equiv 0 \bmod p^k$ and $f'(a) \neq 0 \bmod p$, then there is a unique $g \bmod p$ such as $f(a + gp^k) \equiv 0 \bmod p^{k+1}$.

Numerous repetitions of the above lemma are needed in order to complete a solution of a given equation modulo of higher power which is of course computationally intensive. After every iteration derivative computed roots are required. Thus one hesitates in using the above lemma for the solutions of polynomial congruences with higher power moduli. Root-finding iterative technique is employed to find solutions of linear and quadratic congruences modulo with higher power of a prime p. In particular, secant method is used to elucidate this concept. The following iterative algorithm reveals the concept of Secant Method as reported by (Autar, 2008).

The Secant Method: It is well known that Secant method is more useful then Newton's method because the former method needs iterations without derivative that may be harder in various cases. Assume that two initial estimates x_0 and x_1 are known for the desired root α of $f(x)=0$. The iteration formula for Secant method is

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

In particular, for solving a linear of the form $ax \equiv b\,(\text{mod } p^k)$, where x_k and x_{k+1} are the initial solutions, then by using last equation, x_{k+2} follow the following recursive equation $bx_{k+2} = bx_{k+1} + bx_k - ax_k x_{k+1}$.

As far as the convergence of an *r*th order iterative method is concerned, it affirms that the correctness or precision to calculate the existing estimation x_k is only rk digit. This means that, if algorithm starts with a t-digit integer y_k as the starting approximation modulo p^m, then y_{k+1} would be a new estimation in modulo p^{rm} containing tr-digits.

MATERIAL AND METHODS

In this research work secant method was employed to trial linear and quadratic congruences along with higher degree congruences. Proceeding steps computed a solution mod p^k, based on straight forward translation to the root-finding numerical techniques used for speeding convergence to a real root for polynomials that started with a given solution having higher degree congruences. This grabbed an interesting idea to form speedy algorithms together with the acknowledgement that the root-finding techniques were equally good with the congruence equations over the ring of integers. The *p*-adic convergence was proved using astute proofs. It was proved in Theorem 2, that if x_k, was the solution of the congruence as $ax^2 \equiv b\,(\text{mod } p^{k_1})$ and x_{k+1}, was the solution of the congruence as $ax^2 \equiv b\,(\text{mod } p^{k_2})$ then x_{k+2} was the solution of the congruence as $ax^2 \equiv b\,(\text{mod } p^{k_1+k_2})$ satisfied the equation given as:

$$a(x_k + x_{k+1})x_{k+2} \equiv b + ax_k x_{k+1}\,(\text{mod } p^{k_1+k_2})$$

where a,b and $n>0$ were integers not divisible by a prime p. Theorem 2 was applied recursively such that solutions modulo $p^{k_1+k_2}$ were obtained. On the other hand, modulo higher powers of primes used lifting technique, which required k_1+k_2-1 iterations to reduce the pitfall. The proposed explicit algorithm was not acquired by any sort of derivatives as used in lifting techniques, (this means that the needed derivatives were already incorporated) with some *log k* steps. Results found were concerned to calculate the solutions of congruences of the form $ax^n \equiv b\,(\text{mod } p^k)$, $k \geq 1$, where p was prime and $a,b,n \not\equiv 0\,(\text{mod } p)$ using Secant method by restricting degree to 1 and 2.

The following theorems illustrated the convergence together with solutions of linear and quadratic congruences modulo p^k using Secant method. Before giving the results, rewrite the following two equations.

$$ax^n \equiv b\,(\text{mod } p^k) \quad (1)$$

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

Theorem 1. Let a,b be integers which were not divisible by any prime p and $k \geq 1$. If x_k was the solution of the congruence $ax \equiv b\,(\text{mod } p^k)$ and x_{k+1} was the solution of the congruence was $ax \equiv b\,(\text{mod } p^{k+1})$, then x_{k+2} was the solution of the congruence as $ax \equiv b\,(\text{mod } p^{k+2})$ which satisfied the equation as below:

$$bx_{k+2} = bx_{k+1} + bx_k - ax_k x_{k+1} \quad (3)$$

Proof. Firstly, $f(x) = \frac{b}{x} - a = 0$ was solved using equation (2). This yielded, $bx_{k+2} = bx_{k+1} + bx_k - ax_k ax_{k+1}$. If x_k and x_{k+1} were the solutions of the congruences $ax \equiv b\,(\text{mod } p^k)$ and $ax \equiv b\,(\text{mod } p^{k+1})$ respectively then there existed integers t_1 and t_2 such that $ax_k = b + t_1 p^k$ and $ax_{k+1} = b + t_2 p^{k+1}$ which were put in (3), it yielded $abx_{k+2} = b^2 - t_1 t_2 p^{2k+1}$

$$\equiv b^2\,(\text{mod } p^{k+2})\, since\ 2k+1 \geq k+2\ for\ all\ k \geq 1 \quad (4)$$

Finally, $(b,p)=1$ implied that $(b,p^{k+2})=1$ and hence from (4), it was clear that x_{k+2} was the solution of the congruence as $ax \equiv b\,(\text{mod } p^{k+2})$.

It was interesting to note that using initial estimates modulo p^{k_1} and p^{k_2} instead of p^k and p^{k+1} respectively required less iterations to find the desired solution by means of Secant method. The following theorem illustrated the solution of a quadratic congruence modulo $p^{k_1+k_2}$ using Secant method.

Theorem 2. Let a,b be the integers which were not divisible by an odd prime p and $k \geq 1$. If x_k was the solution of the congruence as $ax^2 \equiv b\,(\text{mod } p^{k_1})$ and x_{k+1}

was the solution of the congruence as $ax^2 \equiv b \,(\bmod\ p^{k_2})$, then x_{k+2} was the solution of the congruence as $ax^2 \equiv b \,(\bmod\ p^{k_1+k_2})$ that satisfied the congruence as given below

$$a(x_k + x_{k+1})x_{k+2} \equiv b + ax_k x_{k+1} \,(\bmod\ p^{k_1+k_2})$$

Proof. To prove this, solved the equation, $f(x) = \dfrac{b}{x^2} - a = 0$ which used equation (2), $b(x_{k+1} + x_k)x_{k+2} = b(x_{k+1}^2 + x_k x_{k+1} + x_k^2) - ax_k^2 x_{k+1}^2.$

As in the proof of Theorem 1, there existed integers t_1 and t_2 such that, $ax_k = b + t_1 p^{k_1}$ and $ax_{k+1} = b + t_2 p^{k_2}$. Substituted the values and simplified into

$$a(x_{k+1} + x_k)x_{k+2} \equiv b + ax_k x_{k+1} \,(\bmod\ p^{k_1+k_2}) \tag{5}$$

Finally, it was proved that x_{k+2} was the solution of the congruence $ax^2 \equiv b \,(\bmod\ p^{k_1+k_2})$. For this rewrite (5),

$$x_{k+2} \equiv \frac{1}{a(x_k + x_{k+1})}(b + ax_k x_{k+1}) \,(\bmod\ p^{k_1+k_2})$$

This implied that

$$x_{k+2}^2 \equiv \frac{1}{a^2(x_{k+1}^2 + x_k^2 + 2x_k x_{k+1})}(b^2 + a^2 x_{k+1}^2 x_k^2 + 2abx_k x_{k+1}) \,(\bmod\ p^{k_1+k_2})$$

Simplified into,

$$ax_{k+2}^2 \equiv \frac{b(2b + t_1 p^{k+1} + t_2 p^k + 2ax_k x_{k+1})}{2b + t_1 p^{k+1} + t_2 p^k + 2ax_k x_{k+1}} \,(\bmod\ p^{k_1+k_2}) \tag{6}$$

Next it was claimed that $2b + 2ax_k x_{k+1} \not\equiv 0 \,(\bmod\ p)$. To prove the assertion it was assumed that, $2b + 2ax_k x_{k+1} \equiv 0 \,(\bmod\ p)$. Since p was an odd prime hence it yielded $b + x_k x_{k+1} \equiv 0 \,(\bmod\ p)$. Then using equation (5), $x_{k+2} \equiv 0 \,(\bmod\ p)$ becomes the solution of the congruence $ax^2 \equiv b \,(\bmod\ p)$ only if p divided b which was a contradiction since $(b, p) = 1$. Hence it was concluded that $2b + 2x_k x_{k+1} \not\equiv 0 \,(\bmod\ p)$. This was further written as $2b + t_1 p^{k+1} + t_2 p^k + 2x_k x_{k+1} \not\equiv 0 \,(\bmod\ p)$ and hence $2b + t_1 p^{k+1} + t_2 p^k + 2x_k x_{k+1} \not\equiv 0 \,(\bmod\ p^{k_1+k_2})$. So by Cancelation law (6) yielded that x_{k+2} was the solution of the congruence as $ax^2 \equiv b \,(\bmod\ p^{k_1+k_2})$.

Remark 1: The technique developed for the solution of polynomial congruences, was equally good for the solutions of similar expressions having negative powers. This was entertained as below.

For the solution of equations of the type, $cx^{-m} \equiv d \,(\bmod\ q^r)$, it was sufficient to find the solutions of $cu^m \equiv d \,(\bmod\ q^r)$, where, $ux \equiv 1 \,(\bmod\ q^r)$. It was found that the roots of above equations were the inverses modulo q^r, in the group of non-zero integers modulo q^r. This asserted the solvability of linear congruence $sz \equiv 1 \,(\bmod\ q^r)$ provided s, was a solution of $cu^m \equiv d \,(\bmod\ q^r)$. But the s, also satisfied $cu^m \equiv d \,(\bmod\ q)$. In other words, $cs^m \equiv d \,(\bmod\ q)$. Since d was not divisible by q, so cu^m was not divisible by either. It followed that u was not divisible by q. Thus u and q were prime to each other. This yielded that the equation $ux \equiv 1 \,(\bmod\ q^r)$ had a solution. Let it be t. Then, t was the desired solution of the congruence $cx^{-m} \equiv d \,(\bmod\ q^r)$.

RESULTS AND DISCUSSION

The p-adic theory of numbers was considered precious to explore many applications in mathematics and computer science since ages. An interesting relation between number theory and numerical analysis was studied, based on Newton's method, which comprised of classical problem for finding the zeros of a polynomial. The problem of division was reduced by using zeros of polynomials to find inverse of a number modulo prime powers. The problem of finding zeros and inverse of numbers was proposed by (Krishnamuthy and Murthy, 1983, Andersen and Jenkins, 2013 and Michal and Xenophontos, 2010) who used division schemes from the classical functional iterative schemes and was extended for the polynomial congruenes. These schemes were compared with the schemes currently used in the high-speed digital computers. Instead of using detrimental schemes given by (Kalantari et al, 1997), which was more efficient scheme based on secant method has also been introduced and compared with existing iterative techniques. (Khalid and Malik, 2012) provided solutions of congruences of the form $ax^n \equiv b(\bmod\ p^k)$, $k \geq 1$ where a, b and n>0 were integers which were not divisible by a prime p using Halley's iterative algorithm. It was observed that the solutions of polynomials of the type $ax^n \equiv b(\bmod\ p^k)$, $k \geq 1$ was calculated reasonably fast using proposed technique. Inductively it meant, a polynomial time algorithm in k, which was the best possible, as the number of bits in the answer was in general proportional to k. Thus polynomial congruences were solved using numerical analysis without using reciprocals of p -adic numbers by means of recursive techniques which was similar to the findings of (Khalid and Ahmad 2014). This was also achieved by giving explicit iteration formulas in equations (3) and (5), for solving the equation $f(x) \equiv 0\ (mod\ p^k)$, when f was a polynomial. By "explicit" it meant that the formulas into which the needed derivatives were already incorporated. For instance, Theorem 1 and Theorem 2 were free from any sort of derivative. On comparison with other techniques, the proposed algorithm needed less iteration to find a solution of modulo higher power of primes which provided such computational techniques using Newton's method but never discussed the computational complexity of these methods. The results and analytical analysis showed that the use of Secant method greatly reduced the computational complexity as compared to other techniques discussed by (Stoer and Bulirsch, 2013). The following example illustrated Theorem 2 which solved a quadratic congruence. This showed that, a modulo power 21 was obtained just in five iterations using proposed technique, whereas the same took 21 iterations when lifting techniques were used like Hensel's Lemma (HL). This was further elaborated by the use of an example given below:

Example 1. Objective was to provide solution of the quadratic congruence $2x^2 \equiv 7\ (mod\ 11^{21})$ .which first solved the congruence $2x^2 \equiv 7\ (mod\ 11)$ and $2x^2 \equiv 7\ (mod\ 11^2)$ which yielded was that formed the initial estimates. Simple calculations revealed that $x \equiv 3,8\ (mod\ 11)$ were the solutions of the congruence was $2x^2 \equiv 7\ (mod\ 11)$. Then by Theorem 1, it was found that $x \equiv 113,8\ (mod\ 11^2)$ were the solution of the congruence was $2x^2 \equiv 7\ (mod\ 11)$. Thus either choose $x_1 = 3$, $x_2 = 113$ or $x_1 = 8$, $x_2 = 8$ as initial estimates. By taking $x_1 = 3$, $x_2 = 113$ and putting it in equation(5), it generated $2.116x_3 \equiv 7 + 2.3.113 (mod\ 11^3)$. Through simplification $x_3 \equiv 1202\ (mod\ 11^3)$ was obtained. Successive application of the same technique yielded the roots of the given congruence modulo $11^3, 11^5$, and so on until the solution of the congruence $2x^2 \equiv 7\ (mod\ 11^{21})$. was obtained. The necessary computations together with Hensel's Lemma (HL) were summarized in the following table.

Table 1. Comparison of Hensel Lemma, and Secant Method.

k	**Methods**	x_k	x_{k+1}	$x_{k+2}\ (\text{mod}\ p^{k_1+k_2})$
1	Secant	3	113	1202 $(\text{mod}\ 11^3)$
	Hensel Lemma	3	113 $(\text{mod}\ 11^2)$	-
2	Secant	113	1202	156929 $(\text{mod}\ 11^5)$
	Hensel Lemma	113	1202 $(\text{mod}\ 11^3)$	-
3	Secant	1202	156929	52820606 $(\text{mod}\ 11^8)$
	Hensel Lemma	1202	4122 $(\text{mod}\ 11^4)$	-
4	Secant	156929	52820606	29612017359708 $(\text{mod}\ 11^{13})$
	Hensel Lemma	4122	4122 $(\text{mod}\ 11^5)$	-
5	Secant	52820606	29612017359708	5531156954935109939642 $(\text{mod}\ 11^{21})$
	Hensel Lemma	4122	326224 $(\text{mod}\ 11^6)$	

Solution of Congruence $2x^2 \equiv 7\ (mod\ 11^{21})$ with $x_1 = 3$ and $x_2 = 113$ as Initial estimates.

Moreover, from the numerical computations of Example 1, it was observed that the time complexity for an ordinary iterative method was similar to Hansel's lemma as reported by (Ivan and Zuckerman, 2005 and David, 2007) was $O(m)$, whereas algorithms developed by proposed method yielded result as $O(log_{k_1+k_2} m)$ for equation (5). Therefore, the techniques suggested in this study performed much faster for values of m in powers of $k_1 + k_2$ in contrast to existing techniques for solving polynomial congruences.

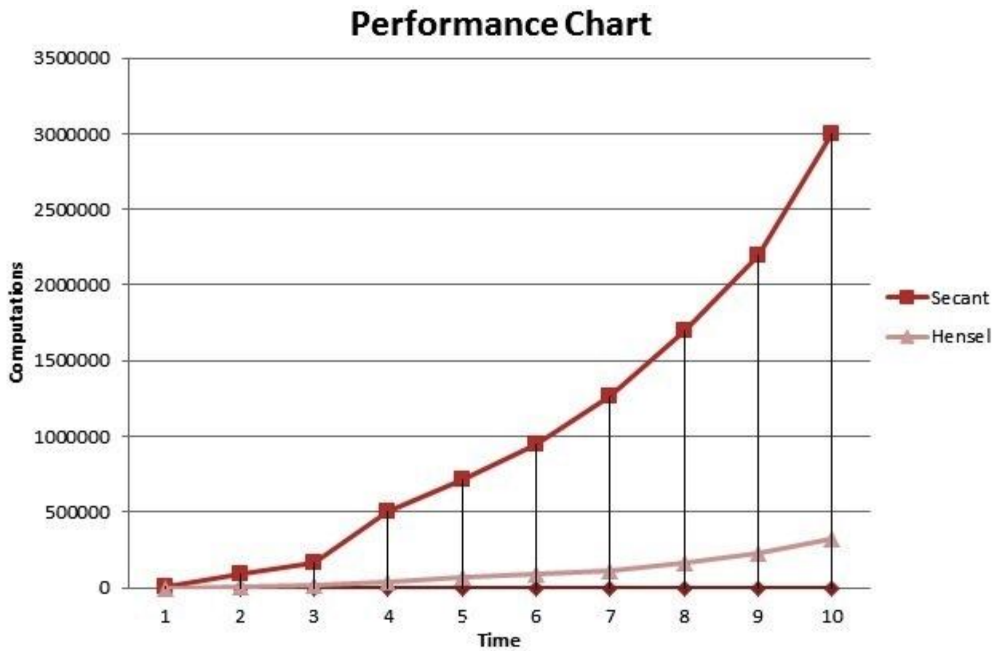

Figure 1 Gives a Comparison between the performance of Hensel lemma and Secant method.

Figure 1 also showed the comparative performance of Suggested method as compared to Hensel lemma in terms of number of computations per unit time. It was seen that just after ten iterations it was above the desired line by means of secant method while the speed of Hensel's lemma was close to the number of iterations. This meant that a solution modulo p^m needed m steps by means of Hensel's lemma whereas it required log (m **)** steps using proposed technique.

REFERENCES

Adler, A., and J.E. Coury (1995). The Theory of Numbers. Jones and Bartlett Publishers; Boston (Massachusetts).

Andersen, N., and P.I. Jenkins (2013). Divisibility properties of coefficients of level p modular functions for genus zero primes. Proceedings of the American Mathematical Society. 141(1): 41-53

Autar, K.K. (2008). Numerical Methods with Applications; Lulo (Florida).

Ben, A.I. (1997). Newton's method with modified functions. Contemp. Math. 204: 39-50

David, M.D. (2007). Elementary Number Theory. Tata McGra-Hill Publishing Company; New Delhi (India).

Eric, B. (2009). Iterative root approximation methods in p-adic Numerical Analysis. Journal of Complexity. 25(6): 511-529

Eugen, V. (2006). Solutions of Some Classes of Congruences. The Teaching of Mathematics. 4 (1): 41-44

Ivan, N., and H. Zuckerman (2008). An introduction to the Theory of Numbers. Wiley India Pvt. Limited.

Kalantari, B., I Kalantari and R. Z. Nahandi (1997). A basic family of iteration functions for polynomial root finding and its characterizations, Journal of Computational and Applied Mathematics, 80(2), 209-226.

Khalid, M. and A. Malik (2012). An Account of Congruences using Halley' Method, World Applied Sciences Journal. 16 (11): 1626-1630

Khalid, M. and F. Ahmad (2014). Recursive Elucidation of Polynomial Congruences Using Root-Finding Numerical Techniques, Abstract and Applied Analysis. 2014: 1-9

Krishnamurthy, E.V., and V.K. Murthy (1983). Fast Iterative Division of P-adic Numbers. IEEE Transactions on Computers. 32: 396-398

Michal, P.K., and C. Xenophontos (2010). Numerical Analysis Meets Number Theory: Using Rootfinding Methods To Calculate Inverses Mod p^n. Appl. Anal. Discrete Math. 4 : 23-31

Stoer, J., and R. Bulirsch (2013). Introduction to numerical analysis. Springer Science & Business Media; USA.

Thomas, C. (2005). Elementry Number Theory with Applications. Academic Press; USA.