BAREKENG: Journal of Mathematics and Its Applications
March 2026 Volume 20 Issue 1 Page 0853–0864
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol20iss1pp0853-0864

HYBRIDIZING HENSEL'S LEMMA, FUNDAMENTAL THEOREM OF ARITHMETIC, AND CHINESE REMAINDER THEOREM FOR SOLVING POLYNOMIAL CONGRUENCES

Eka Oktaviansyah[1], Edi Kurniadi[2*], Dianne Amor Kusuma[3]

[1]*Mathematics Bachelor Degree Program, Faculty of Mathematics and Natural Sciences, Universitas Padjadjaran*
[2,3]*Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Padjadjaran*
Jln. Raya Bandung Sumedang Km 21, Jatinangor, Sumedang 45363, Indonesia

*Corresponding author's e-mail: * **edi.kurniadi@ unpad.ac.id***

Article Info

Article History:

Received: 16th June 2025
Revised: 15th July 2025
Accepted: 29th July 2025
Available online: 24th November 2025

Keywords:

Chinese Remainder Theorem;
Computational number theory;
Fundamental Theorem of Arithmetic;
Hensel's Lemma;
Polynomial congruence;
Recursive formula.

ABSTRACT

Polynomial congruence can be solved by applying Hensel's Lemma. However, Hensel's Lemma itself does not apply to solving generalized polynomial congruences. The purpose of this research is to determine the recursive formula for the solution of polynomial congruence modulo prime numbers and to construct a general solution algorithm of polynomial congruence modulo arbitrary positive integers. Unlike previous studies, this research proposes the recursive hybrid algorithm combining Hensel's Lemma, the Fundamental Theorem of Arithmetic, and the Chinese Remainder Theorem, highlighting the originality of the approach in extending its application beyond prime power moduli. The result of this research is the form of a recursive formula for the solution of polynomial congruence modulo prime numbers and the algorithm for solving polynomial congruence modulo arbitrary positive integers using the combination of Hensel's Lemma, Fundamental Theorem of Arithmetic, and Chinese Remainder Theorem. The results of this research contribute to the development of mathematical methods, especially in the field of number theory. However, the applicability of the recursive formula is limited to cases where the conditions of Hensel's Lemma are satisfied, that is, when a solution of the polynomial modulo a prime is such that the polynomial equals zero while its derivative does not equal zero modulo the same prime. Extending the method to situations where this condition fails remains a subject for future research.

How to cite this article:

E. Oktaviansyah, E. Kurniadi, and D. A. Kusuma, "HYBRIDIZING HENSEL'S LEMMA, FUNDAMENTAL THEOREM OF ARITHMETIC, AND CHINESE REMAINDER THEOREM FOR SOLVING POLYNOMIAL CONGRUENCES", *BAREKENG: J. Math. & App.*, vol. 20, iss. 1, pp. 0853-0864, Mar, 2026.

Journal homepage: *https://ojs3.unpatti.ac.id/index.php/barekeng/*
Journal e-mail: *barekeng.math@yahoo.com; barekeng.journal@mail.unpatti.ac.id*

Research Article · Open Access

1. INTRODUCTION

The branch of mathematics that studies the properties of integers is called number theory. One concept often used in number theory is congruence, introduced by Carl Friedrich Gauss in 1801 [1]. Congruence uses a modular arithmetic calculation system that expresses the remainder of the division of an integer by another integer [2]. Thue states that Thue's equation, the Diophantine equation $F(x,y) = r$, where $F(x,y)$ is an irreducible homogeneous polynomial function of degree $n \geq 3$, and r is a nonzero rational number, has infinite solutions for x and y [3],[4],[5]. The results show that by using Thue's equation, researchers can further find various formulas for solving polynomial equations. With this formula, mathematical models that often use a system of polynomial equations can be solved more efficiently [6],[7],[8]. A Diophantine equation is an equation with integer coefficients that has an integer solution [9] (p. 119). Matiyasevich proved that no formula can generally solve the Diophantine equation [4]. However, research to solve the Diophantine equation is still being done, such as Grechuk's research that can determine the solution of a bounded Diophantine polynomial equation [5]. In addition, Mosunov, through his research, determined the upper bound of the number of solutions of the Diophantine polynomial equation using the Thue-Mahler equation [10],[11].

The solution of the congruence $ax \equiv c \pmod{m}$ is identical to the integer solutions x and y of the Diophantine equation $ax = my + c$ [9]. Therefore, an infinite number of solutions of the Diophantine polynomial equation results in an infinite solutions of the polynomial congruence. This statement is supported by the results of Gherga and Siksek, who stated that the number of polynomial congruence solutions is infinite [11]. These results are significant in modular arithmetic calculation systems because researchers can further study ways to solve polynomial congruences. For instance, Chinburg et al. [12], as well as Koppanati and Kumar [13], demonstrated that extending congruence solving beyond linear and quadratic cases to cubic and higher-degree polynomial congruences enables secure encryption of multimedia content in the cloud, showing the practical importance of polynomial congruences in strengthening modern cryptographic systems. In quantum cryptography, polynomial-based hashing methods have been shown to rely on number-theoretic properties of polynomial congruences, enabling efficient authentication and strengthening key distribution protocols [14]. Another relevant research was conducted by Ghosal [15], who said that number theory is one of the most important areas of Mathematics used in Computer Science and the basis behind the science of modern Cryptography. The research conducted was to study the development and application of number theory. The aim was to review the history of number theory and explore its influence on production, everyday life, and its application in engineering. The research found that number theory and modern computing technology can provide exciting solutions to real-life problems.

In his research, Chan and Chen [16] used circular argumentation on the proof of Euclid's theorem related to the infinity of prime numbers underlying the Fundamental Theorem of Arithmetic. The argumentation is determined by carefully observing the prime numbers analyzed in the statement. The result of his research, identifying the Fundamental Theorem of Arithmetic (FTA) as Unique Prime Factorization over S (UPF-S) for some set S of prime numbers, shows that FTA for natural numbers holds if and only if the set S is infinite and contains all prime numbers. Ahmad et al. [17] have investigated the parameters that affect the performance of Chinese Remainder Theorem (CRT) compression. In the investigation, experiments were conducted on the KODAK data set. The analysis was to correlate the decrease in CRT compression performance with the number of modules, that is, the size of the compressed block. The analysis showed that the performance improved at fewer modules, achieving an average compression ratio of 8% on the KODAK data set.

Alhassan et al. [18] attempted to identify some algebraic properties of the CRT. CRT is an essential mathematical theorem for solving simultaneous equations related to different moduli. CRT also makes it possible to reconstruct integers within a specific range from the modulo of their residues to the relative modulo of pairwise primes and code sets of structures for manipulations on huge integers. The results of his research identified that the Prime and Ring Ideal Domain statements can be classified as some algebraic properties of the Chinese Remainder Theorem. According to Weiss [19], constructing real numbers involves creating an equivalence class of the Cauchy rational number sequence concerning ordinary absolute values. A completely different set of numbers, better known as *p*-adic numbers, can be constructed using different absolute values. So, with this basic description of the finite extension of *p*-adic numbers, the reader can explain the algebraic closure of the field of *p*-adic numbers. This field is incomplete, so a further step is needed to find a field containing *p*-adic numbers that is complete and algebraically closed. Furthermore, with such a field, many options, including the analysis of *p*-adic numbers, are open to researchers.

Based on the explanation above, previous research results show that gaps still need to be developed further, and no one has made a hybrid algorithm, which is a combination of Hensel's Lemma, the Fundamental Theorem of Arithmetic, and the Chinese Remainder Theorem. Previous studies have only examined certain parts of Hensel's Lemma, the Fundamental Theorem of Arithmetic, and the Chinese Remainder Theorem, and have not combined them to find a hybrid algorithm. From these studies, new problems arise related to the form of the recursive formula for the solution of the congruence of polynomials modulo prime numbers and the general solution algorithm of polynomial congruence modulo arbitrary positive integers. This result is simpler to find the solution of the congruence of polynomials modulo prime numbers compared to the previous result. Therefore, in this research, the recursive formula for the solution of the congruence of polynomials modulo prime numbers using Hensel's Lemma is determined. In addition, the solution algorithm of polynomial congruence modulo arbitrary positive integers using Hensel's Lemma is determined. A combination of Hensel's Lemma, the Fundamental Theorem of Arithmetic, and the Chinese Remainder Theorem is used to construct the solution algorithm of polynomial congruence modulo arbitrary positive integers.

2. RESEARCH METHODS

This research is classified as theoretical development research in the field of mathematics, aimed at developing a recursive formula for the solution of the congruence of polynomials modulo prime numbers and constructing a general solution algorithm of polynomial congruence modulo arbitrary positive integers. The primary research instruments are a literature review and a theoretical analysis of key mathematical definitions and theorems, including *p*-adic integers, polynomial ring, Hensel's Lemma, the Fundamental Theorem of Arithmetic, and the Chinese Remainder Theorem. These provide the conceptual framework that supports the development of the proposed method. Since no empirical data are collected, this research relies on deductive reasoning through mathematical proof and validation through illustrative polynomial congruence cases that demonstrate the proposed algorithm.

2.1 *p*-adic Integers

Definition 1 [20]. *If p is prime, then a p-adic integer can be defined as the series*

$$a = \sum_{i=k}^{\infty} s_i p^i = s_k p^k + s_{k+1} p^{k+1} + s_{k+2} p^{k+2} + \cdots, \tag{1}$$

where $0 \leq k \in \mathbb{Z}$ *and* $0 \leq s_i < p, s_i \in \mathbb{Z}$.

Definition 2 [20]. *If p is prime, then the p-adic integers can be defined as the sequence*

$$a = (a_0 \ (mod\ p), a_1 \ (mod\ p^2), a_2 \ (mod\ p^3), a_3 \ (mod\ p^4), \ldots) \tag{2}$$

where $a_{i-1} \equiv a_j \ (mod\ p^i), i \leq j$.

Definition 3 [20]. *The set of all p-adic integers is called* $\mathbb{Z}_p$.

Example 1. Suppose $p = 3$. We want to express the integer 7 in its 3-adic form. First, observe that

$$7 \equiv 1^2 \ (\text{mod } 3).$$

Although $7 \not\equiv 1^2 \ (\text{mod } 3^2)$, we can replace 1 with $1 + 3$, since $1 \equiv (1 + 3) \ (\text{mod } 3)$. Thus,

$$7 \equiv (1 + 3)^2 \ (\text{mod } 3^2).$$

Continuing this process, as we lift the solution to higher powers of 3, we obtain:

$$7 \equiv (1 + 3 + 3^2)^2 \ (\text{mod } 3^3),$$

$$7 \equiv (1 + 3 + 3^2)^2 \ (\text{mod } 3^4),$$

$$7 \equiv (1 + 3 + 3^2 + 2 \cdot 3^4)^2 \ (\text{mod } 3^5),$$

$$7 \equiv (1 + 3 + 3^2 + 2 \cdot 3^4)^2 \ (\text{mod } 3^5),$$

$$7 \equiv (1 + 3 + 3^2 + 2 \cdot 3^4)^2 \ (\text{mod } 3^7),$$

$$7 \equiv (1+3+3^2+2\cdot 3^4+2\cdot 3^7)^2 \pmod{3^8},$$
$$7 \equiv (1+3+3^2+2\cdot 3^4+2\cdot 3^7+3^8)^2 \pmod{3^9},$$
$$7 \equiv (1+3+3^2+2\cdot 3^4+2\cdot 3^7+3^8+3^9)^2 \pmod{3^{10}},$$
$$7 \equiv (1+3+3^2+2\cdot 3^4+2\cdot 3^7+3^8+3^9+2\cdot 3^{10})^2 \pmod{3^{11}}.$$

If this process is carried out indefinitely, we obtain that 7 can be expressed as the perfect square of a 3-adic number, namely

$$7 = (1+3+3^2+2\cdot 3^4+2\cdot 3^7+3^8+3^9+2\cdot 3^{10}+\cdots)^2$$

in $\mathbb{Z}_3$.

2.2 Polynomial Ring

Definition 4 [21]. *Suppose R is a commutative ring. The set $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 | a_i \in R, 0 \leq n \in \mathbb{Z}\}$ is a polynomial ring.*

Theorem 1. *Suppose p is a prime number. If $f(x) \in \mathbb{Z}_p[x]$ and $y \in \mathbb{Z}_p$, then it holds*

$$f(x+y) = f(x) + f'(x)y + g(x,y)y^2 \tag{3}$$

with $g(x,y) \in \mathbb{Z}_p[x,y]$.

Proof. Given $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}_p[x]$ and $y \in \mathbb{Z}_p$. It will be proved that $f(x+y) = f(x) + f'(x)y + g(x,y)y^2$ with $g(x,y) \in \mathbb{Z}_p[x,y]$. Based on what has been known, obtained

$$\begin{aligned}
f(x+y) &= \sum_{i=0}^{d} a_i (x+y)^i \\
&= a_0 + a_1(x+y) + a_2(x+y)^2 + a_3(x+y)^3 + \cdots \\
&= a_0 + a_1 x + a_1 y + a_2(x^2 + 2xy + y^2) + a_3(x^3 + 3x^2 y + 3xy^2 + y^3) + \cdots \\
&= a_0 + a_1 x + a_1 y + a_2 x^2 + 2a_2 xy + a_2 y^2 + a_3 x^3 + 3a_3 x^2 y + 3a_3 xy^2 + a_3 y^3 + \cdots \\
&= a_0 + (a_1 x + a_2 x^2 + a_3 x^3) + (a_1 y + 2a_2 xy + 3a_3 x^2 y) + a_2 y^2 + 3a_3 xy^2 + a_3 y^3 + \cdots \\
&= a_0 + \sum_{i=1}^{d} a_i x^i + \sum_{i=1}^{d} i a_i x^{i-1} y + \sum_{i=1}^{d} a_i g_i(x,y) y^2 \\
&= \sum_{i=0}^{d} a_i x^i + \sum_{i=1}^{d} i a_i x^{i-1} y + \sum_{i=1}^{d} a_i g_i(x,y) y^2 \\
&= f(x) + f'(x)y + g(x,y)y^2,
\end{aligned}$$

with $g(x,y) = \sum_{i=1}^{d} a_i g_i(x,y) \in \mathbb{Z}_p[x,y]$. So, it is proven that $f(x+y) = f(x) + f'(x)y + g(x,y)y^2$, with $g(x,y) \in \mathbb{Z}_p[x,y]$. ■

2.3 Hensel's Lemma

Lemma 1 [20]. *Suppose p is a prime number. If $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ satisfy $f(a) \equiv 0 \ (mod\ p)$ and $f'(a) \not\equiv 0 \ (mod\ p)$, then there exists a unique $\alpha \in \mathbb{Z}_p$ such that*

$$f(\alpha) = 0 \ and \ \alpha \equiv a \ (mod\ p). \tag{4}$$

Example 2. Suppose $p = 2$ and $f(x) = x^3 - 5 \in \mathbb{Z}_2[x]$. Suppose $a = 1 \in \mathbb{Z}_2$. Obtained $f(1) = 1^3 - 5 = -4 \equiv 0 \pmod 2$ and $f'(1) = 3 \cdot 1^2 = 3 \equiv 1 \pmod 2$. Because it satisfies $f(1) \equiv 0 \pmod 2$ and $f'(1) \not\equiv 0 \pmod 2$, by Lemma 1, there exists a unique $\alpha \in \mathbb{Z}_2$ such that $f(\alpha) = 0$ and $\alpha \equiv 1 \pmod 2$.

For example, $a_1 \equiv a \equiv 1 \pmod 2$. Find $a_n \in \mathbb{Z}_2$ such that $a_n^3 - 5 \equiv 0 \pmod{2^n}$ and $a_n \equiv 1 \pmod 2$ for every $n > 1$. Obtained,

$$0 \equiv (1^3 - 5) \pmod{2^2} \text{ and } 1 \equiv 1 \pmod 2,$$
$$0 \equiv ((1+2^2)^3 - 5) \pmod{2^3} \text{ and } (1+2^2) \equiv 1 \pmod 2,$$
$$0 \equiv ((1+2^2+2^3)^3 - 5) \pmod{2^4} \text{ and } (1+2^2+2^3) \equiv 1 \pmod 2,$$

$$0 \equiv ((1+2^2+2^3+2^4)^3-5)(\text{mod } 2^5) \text{ and } (1+2^2+2^3+2^4) \equiv 1(\text{mod } 2),$$
$$0 \equiv ((1+2^2+2^3+2^4)^3-5)(\text{mod } 2^6) \text{ and } (1+2^2+2^3+2^4) \equiv 1(\text{mod } 2).$$

Therefore, it is obtained

$$a_2 \equiv 1 \ (\text{mod } 2^2),$$
$$a_3 \equiv (1+2^2) \ (\text{mod } 2^3),$$
$$a_4 \equiv (1+2^2+2^3) \ (\text{mod } 2^4),$$
$$a_5 \equiv (1+2^2+2^3+2^4) \ (\text{mod } 2^5),$$
$$a_6 \equiv (1+2^2+2^3+2^4) \ (\text{mod } 2^6),$$
$$\vdots$$

So, $\alpha = 1+2^2+2^3+2^4+\cdots$.

2.4 Fundamental Theorem of Arithmetic

In this subsection, decomposition of any positive integer into prime numbers, linear congruence, and Chinese Remainder Theorem, and an algorithm to find a recursive formula are recalled. It started with the following theorem.

Theorem 2 [22]. *Every positive integer can be singularly expressed as a multiplication of prime numbers*.

This theorem states that for any integer $n > 1$, there exists a unique sequence of prime numbers $(p_1, p_2, \dots, p_k)$ and corresponding positive integers $(e_1, e_2, \dots, e_k)$ such that:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}.$$

Example 3. The number 152 can be expressed as $152 = 2^3 \cdot 19$. No other combination of prime numbers will yield 152.

2.5 Chinese Remainder Theorem

Definition 5 [23]. *An equation of the form $ax \equiv b \ (mod \ n)$ is a linear congruence*.

Theorem 3 [23]. *Suppose $n_1, n_2, \dots, n_r$ a positive integer with $gcd(n_i, n_j) = 1$ for $i \neq j$. Then the linear congruence system*

$$x \equiv a_1 \ (mod \ n_1)$$
$$x \equiv a_2 \ (mod \ n_2)$$
$$\vdots$$
$$x \equiv a_r \ (mod \ n_r)$$

has a unique solution modulo $n_1 n_2 \dots n_r$.

3. RESULTS AND DISCUSSION

This section contains the research results, which include the recursive formula of the solution of the congruence of polynomials modulo prime numbers by using Hensel's Lemma and the algorithm for solving the congruence of polynomials modulo arbitrary positive integers by using a combination of Hensel's Lemma, the Fundamental Theorem of Arithmetic, and the Chinese Remainder Theorem.

The first result obtained in this study is given in Proposition 1, and the second result in this study is related to the algorithm for solving polynomial congruence modulo arbitrary positive integers using the combination of Hensel's Lemma, the Fundamental Theorem of Arithmetic, and the Chinese Remainder Theorem.

3.1 Modification of Hensel's Lemma

The first result in this study is Proposition 1, a modification of Hensel's Lemma in Lemma 1. The proof of Proposition 1 is given in detail and is accompanied by an example.

Proposition 1. *Suppose p is a prime number. If $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ satisfy $f(a) \equiv 0 \ (mod\ p)$ and $f'(a) \not\equiv 0 \ (mod\ p)$, then for every $a_{m-1} \in \mathbb{Z}_p$, where $m \in \mathbb{Z}$ with $m \geq 2$, holds*

$$a_{m-1} \equiv \left(a_{m-2} + f(a_{m-2})(-f'(a)^{-1})\right) (\text{mod } p^m) \tag{5}$$

with $a_0 \equiv a \ (\text{mod } p)$.

Proof. Let p be a prime number and $m \in \mathbb{Z}$ with $m \geq 0$. Suppose $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ satisfy $f(a) \equiv 0 \ (\text{mod } p)$ and $f'(a) \not\equiv 0 \ (\text{mod } p)$. By Lemma 1, there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv a \ (\text{mod } p)$. Since $\alpha \in \mathbb{Z}_p$, by Definition 1, α can be represented as a p-adic integer according to Eq. (1), namely $\alpha = \sum_{i=k}^{\infty} s_i p^i = s_k p^k + s_{k+1} p^{k+1} + s_{k+2} p^{k+2} + \cdots$, where $0 \leq k \in \mathbb{Z}$ and $0 \leq s_i < p, s_i \in \mathbb{Z}$. Suppose $k = 0$, it is obtained $\alpha = \sum_{i=0}^{\infty} s_i p^i = s_0 + s_1 p + s_2 p^2 + \cdots$, where $0 \leq s_i < p, s_i \in \mathbb{Z}$.

Let

$$a_m = \sum_{i=0}^{m} s_i p^i = s_0 + s_1 p + s_2 p^2 + \cdots + s_m p^m \,, \tag{6}$$

where $a_m \in \mathbb{Z}_p, 0 \leq s_i < p, s_i \in \mathbb{Z}$. For illustration, suppose some values of m of Eq. (6) as follows:

For $m = 0$, obtained $a_0 = s_0$.

For $m = 1$, obtained $a_1 = s_0 + s_1 p$.

For $m = 2$, obtained $a_2 = s_0 + s_1 p + s_2 p^2$.

For $m = 3$, obtained $a_3 = s_0 + s_1 p + s_2 p^2 + s_3 p^3$.

Therefore, for m, which is increasing, the value of α can be written as $\alpha = \lim_{m \to \infty} a_m$. In addition, based on Definition 2, α can be represented as a sequence

$$\alpha = (a_0 \ (\text{mod } p), a_1 \ (\text{mod } p^2), a_2 \ (\text{mod } p^3), \ldots, a_{m-1} (\text{mod } p^m), \ldots) \tag{7}$$

Because $f(\alpha) = 0$ dan $\alpha \equiv a \ (\text{mod } p)$, it means that for every $m \geq 1$, holds $f(a_{m-1}) \equiv 0 \ (\text{mod } p^m)$ and $a_{m-1} \equiv a \ (\text{mod } p)$.

For $m = 1$, obtained $f(a_0) \equiv 0 \ (\text{mod } p)$ and $a_0 \equiv a \ (\text{mod } p)$.

For $m \geq 2$, suppose

$$a_{m-1} \equiv (a_{m-2} + s_{m-1} p^{m-1}) \ (\text{mod } p^m) \tag{8}$$

with $s_{m-1} \in \mathbb{Z}_p$. Based on Hensel's Lemma, we get

$$f(a_{m-1}) \equiv f(a_{m-2} + s_{m-1} p^{m-1}) \equiv 0 \ (\text{mod } p^m). \tag{9}$$

Since $f(x) \in \mathbb{Z}_p[x]$, based on Theorem 1, it is obtained that

$$f(x + y) = f(x) + f'(x)y + g(x, y)y^2, \qquad g(x, y) \in \mathbb{Z}_p[x, y] \tag{10}$$

By substituting x with a_{m-2} and y with $s_{m-1} p^{m-1}$ in Eq. (10), then obtained

$$f(a_{m-2} + s_{m-1} p^{m-1}) = f(a_{m-2}) + f'(a_{m-2}) s_{m-1} p^{m-1} + z s_{m-1}^2 p^{m-2} p^m. \tag{11}$$

where $z = g(a_{m-2}, s_{m-1} p^{m-1}) \in \mathbb{Z}_p$.

By performing modulo reduction p^m in Eq. (11), we obtain

$$f(a_{m-2} + s_{m-1} p^{m-1}) \equiv (f(a_{m-2}) + f'(a_{m-2}) s_{m-1} p^{m-1}) \ (\text{mod } p^m). \tag{12}$$

Next, substituting Eq. (12) into Eq. (9), we get

$$f(a_{m-2}) + f'(a_{m-2}) s_{m-1} p^{m-1} \equiv 0 \ (\text{mod } p^m),$$

$$s_{m-1}p^{m-1} \equiv -f(a_{m-2})f'(a_{m-2})^{-1} \pmod{p^m}. \quad (13)$$

Since $f(a_{m-2}) \in \mathbb{Z}_p$, $f(a_{m-2})$ has an inverse of addition, that is, $-f(a_{m-2}) \in \mathbb{Z}_p$. To prove the existence of $f'(a_{m-2})^{-1}$ as the inverse of multiplication, it will first be shown that $f'(a_{m-2}) \equiv f'(a)$. It is known that $a_{m-2} \equiv a \pmod{p}$. Therefore, it is obtained

$$a_{m-2} \equiv a \pmod{p} \Rightarrow f'(a_{m-2}) \equiv f'(a) \not\equiv 0 \pmod{p} \quad (14)$$

Based on Eq. (14), $f'(a_{m-2}) \not\equiv 0 \pmod{p}$. This means, $f'(a_{m-2}) \in \mathbb{Z}_p^*$. Since $f'(a_{m-2}) \in \mathbb{Z}_p^*$, $f'(a_{m-2})$ has a multiplication inverse, that is, $f'(a_{m-2})^{-1} \in \mathbb{Z}_p^*$. Therefore, it is proven that $-f(a_{m-2}) \in \mathbb{Z}_p$ and $f'(a_{m-2})^{-1} \in \mathbb{Z}_p^*$.

Furthermore, by substituting Eq. (14) into Eq. (13), we obtain

$$s_{m-1}p^{m-1} \equiv -f(a_{m-2})f'(a)^{-1} \pmod{p^m}. \quad (15)$$

By substituting Eq. (15) into Eq. (8), we obtain

$$a_{m-1} \equiv \left(a_{m-2} + \left(-f(a_{m-2})\right)f'(a)^{-1}\right) \pmod{p^m} \quad (16)$$

Since $\mathbb{Z}_p$ is a commutative ring, Eq. (16) becomes

$$a_{m-1} \equiv \left(a_{m-2} + f(a_{m-2})(-f'(a)^{-1})\right) \pmod{p^m}.$$

So, it is proven that for every $m \geq 2$ holds $a_{m-1} \equiv (a_{m-2} + f(a_{m-2})(-f'(a)^{-1}))(\text{mod } p^m)$ with $a_0 \equiv a \pmod{p}$. ■

Example 4. Suppose $p = 3$ and $f(x) = 2x^2 + 1 \in \mathbb{Z}_3[x]$. Suppose $a = 1 \in \mathbb{Z}_3$. We obtain $f(1) = 2 \cdot 1^2 + 1 = 3 \equiv 0 \pmod{3}$ and $f'(1) = 4 \cdot 1 = 4 \equiv 1 \pmod{3}$. Since it satisfies $f(1) \equiv 0 \pmod{3}$ and $f'(1) \not\equiv 0 \pmod{3}$, by Proposition 1, for every $a_{m-1} \in \mathbb{Z}_p$, where $m \in \mathbb{Z}$ with $m \geq 2$, holds

$$\begin{aligned} a_{m-1} &\equiv (a_{m-2} + f(a_{m-2})(-f'(1)^{-1}))(\text{mod } 3^m) \\ &\equiv (a_{m-2} + f(a_{m-2})(-1^{-1}))(\text{mod } 3^m) \\ &\equiv (a_{m-2} + f(a_{m-2}) \cdot 2)(\text{mod } 3^m), \end{aligned}$$

with $a_0 \equiv 1 \pmod{3}$.

For $m = 2$, obtained

$$\begin{aligned} a_1 &\equiv (a_0 + f(a_0) \cdot 2) \equiv (1 + f(1) \cdot 2) \pmod{3^2} \\ &\equiv (1 + 3 \cdot 2) \pmod{3^2} \\ &\equiv 7 \pmod{3^2}. \end{aligned}$$

For $m = 3$, obtained

$$\begin{aligned} a_2 &\equiv (a_1 + f(a_1) \cdot 2) \equiv (7 + f(7) \cdot 2) \pmod{3^3} \\ &\equiv (7 + 18 \cdot 2) \pmod{3^3} \\ &\equiv 43 \pmod{3^3} \\ &\equiv 16 \pmod{3^3}. \end{aligned}$$

3.2 Polynomial Congruence Solving Algorithm

The second result in this research is related to the algorithm for solving polynomial congruence modulo arbitrary positive integers using a combination of Hensel's Lemma, the Fundamental Theorem of Arithmetic, and the Chinese Remainder Theorem. If given a polynomial congruence modulo arbitrary positive integers, the solution can be determined using the combination of Hensel's Lemma, Fundamental Theorem of Arithmetic, and Chinese Remainder Theorem with the following algorithm:

1. Factorize the modulo of a polynomial congruence using the Fundamental Theorem of Arithmetic.
2. Determine the solution of the polynomial congruence for each modulo prime number.
3. Check whether the solution satisfies the conditions of Hensel's Lemma.

4. Apply the recursive formula of Hensel's Lemma to determine the solution of a polynomial congruence modulo p^m.
5. Apply the Chinese Remainder Theorem to determine the initial modulo polynomial congruence solution.

The application of the algorithm for solving polynomial congruence using the combination of Hensel's Lemma, the Fundamental Theorem of Arithmetic, and the Chinese Remainder Theorem is given in Example 5.

Example 5. Suppose $f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod{2601}$. To solve $f(x)$ using Hensel's Lemma, the modulo of the polynomial congruence is factorized using the Fundamental Theorem of Arithmetic. Therefore, it is obtained:

$$f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod{3^2 \cdot 17^2} \tag{17}$$

Split the polynomial congruence in Eq. (17) into:

$$f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod{3^2} \tag{18}$$

$$f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod{17^2} \tag{19}$$

After obtaining the form of a polynomial congruence modulo p^m, the next step is to determine the solution of the polynomial congruence modulo p by substituting each element into Eqs. (18) and (19) as shown in Table 1 and Table 2.

Table 1. Values of x and $f(x) \pmod 3$, with $f(x) = 2x^3 - 9x^2 + 17x - 6$

x	$f(x) \pmod 3$
0	$f(0) \equiv 0 \pmod 3$
1	$f(1) \equiv 1 \pmod 3$
2	$f(2) \equiv 2 \pmod 3$

Based on Table 1, the solution of the polynomial congruence $f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod 3$ is $a \equiv 0 \pmod 3$.

Table 2. Values x and $f(x) \pmod{17}$, with $f(x) = 2x^3 - 9x^2 + 17x - 6$

x	$f(x) \pmod{17}$	x	$f(x) \pmod{17}$
0	$f(0) \equiv 11 \pmod{17}$	9	$f(9) \equiv 9 \pmod{17}$
1	$f(1) \equiv 4 \pmod{17}$	10	$f(10) \equiv 6 \pmod{17}$
2	$f(2) \equiv 8 \pmod{17}$	11	$f(11) \equiv 3 \pmod{17}$
3	$f(3) \equiv 1 \pmod{17}$	12	$f12 \equiv 12 \pmod{17}$
4	$f(4) \equiv 12 \pmod{17}$	13	$f(13) \equiv 11 \pmod{17}$
5	$f(5) \equiv 2 \pmod{17}$	14	$f(14) \equiv 12 \pmod{17}$
6	$f(6) \equiv 0 \pmod{17}$	15	$f(15) \equiv 10 \pmod{17}$
7	$f(7) \equiv 1 \pmod{17}$	16	$f(16) \equiv 0 \pmod{17}$
8	$f(8) \equiv 0 \pmod{17}$		

Based on Table 2, the solution of the polynomial congruence $f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod{17}$ is $a \equiv 6 \pmod{17}$, $b \equiv 8 \pmod{17}$, and $c \equiv 16 \pmod{17}$.

To see whether the solutions of the polynomial congruence modulo p satisfy the condition of Hensel's Lemma, the first derivative of the polynomial function of Eq. (17) is determined:

$$f'(x) = 6x^2 - 18x + 17 \tag{20}$$

Substitute the solutions of the polynomial congruence modulo p into (20):

$$f'(0) = 6 \cdot 0^2 - 18 \cdot 0 + 17 \equiv 2 \not\equiv 0 \pmod 3,$$

$$f'(6) = 6 \cdot 6^2 - 18 \cdot 6 + 17 \equiv 6 \not\equiv 0 \pmod{17},$$

$$f'(8) = 6 \cdot 8^2 - 18 \cdot 8 + 17 \equiv 2 \not\equiv 0 \pmod{17},$$

$$f'(16) = 6 \cdot 16^2 - 18 \cdot 16 + 17 \equiv 7 \not\equiv 0 \pmod{17}.$$

Based on these results, it can be stated that each solution of polynomial congruence modulo p satisfies the conditions of Hensel's Lemma.

The solution of the polynomial congruence $f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod 3$ is $a \equiv 0 \pmod 3$ and the first derivative of the function $f(x)$ at that point is $f'(0) \equiv 2 \pmod 3$. In addition, the solution of the polynomial congruence $f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod{17}$ is $a \equiv 6 \pmod{17}$, $b \equiv 8 \pmod{17}$, and $c \equiv 16 \pmod{17}$ and the first derivative of the function $f(x)$ at each of these points is $f'(6) \equiv 6 \pmod{17}$, $f'(8) \equiv 2 \pmod{17}$, and $f'(16) \equiv 7 \pmod{17}$.

Substitute the solution $a \equiv 0 \pmod 3$ into Eq. (5), then the following are obtained:

$$a_0 \equiv 0 \pmod 3,$$

$$a_1 \equiv \left(a_0 + f(a_0)(-f'(0)^{-1})\right) \equiv \left(0 + f(0) \cdot (-2^{-1})\right) \equiv (0 + 3 \cdot 4) \pmod{3^2}$$

$$\equiv 12 \equiv 3 \pmod{3^2}.$$

Based on this calculation, the solution of $f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod{3^2}$ is $a_1 \equiv 3 \pmod{3^2}$.

Substitute the solution $a \equiv 6 \pmod{17}$ to Eq. (5), we get

$$a_0 \equiv 6 \pmod{17},$$

$$a_1 \equiv \left(a_0 + f(a_0)(-f'(6)^{-1})\right) \equiv \left(6 + f(6) \cdot (-6^{-1})\right) \pmod{17^2}$$

$$\equiv (6 + 204 \cdot 48) \equiv (6 + 9792) \equiv 9798 \equiv 261 \pmod{17^2}.$$

Substitute the solution $b \equiv 8 \pmod{17}$ to Eq. (5), we get

$$b_0 \equiv 8 \pmod{17},$$

$$b_1 \equiv \left(b_0 + f(b_0)(-f'(8)^{-1})\right) \equiv \left(8 + f(8) \cdot (-2^{-1})\right) \pmod{17^2}$$

$$\equiv (8 + 0 \cdot 144) \equiv 8 \pmod{17^2}.$$

Substitute the solution $c \equiv 16 \pmod{17}$ to Eq. (5), we get

$$c_0 \equiv 16 \pmod{17},$$

$$c_1 \equiv \left(c_0 + f(c_0)(-f'(16)^{-1})\right) \equiv \left(16 + f(16) \cdot (-7^{-1})\right) \pmod{17^2}$$

$$\equiv (16 + 85 \cdot 165) \equiv (16 + 14025) \equiv 14041 \equiv 169 \pmod{17^2}.$$

Based on this calculation, the solution of $f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod{17^2}$ is $a_1 \equiv 261 \pmod{17^2}$,$b_1 \equiv 8 \pmod{17^2}$and $c_1 \equiv 169 \pmod{17^2}$.

To determine the solution modulo 2601, three linear congruence systems are formed as given in Table 3.

Table 3. List of Linear Congruence Systems to Solve $f(x) \equiv 0 \pmod{2601}$

System	Linear Congruences
1	$x \equiv 3 \pmod{3^2}$, $x \equiv 261 \pmod{17^2}$
2	$x \equiv 3 \pmod{3^2}$, $x \equiv 8 \pmod{17^2}$
3	$x \equiv 3 \pmod{3^2}$, $x \equiv 169 \pmod{17^2}$

Since 3^2 and 17^2 are relatively prime, each linear congruence system in Table 3 has a unique solution modulo $2601 = 3^2 \cdot 17^2$ by Theorem 3.

Let

$$N_1 = \frac{2601}{3^2} = \frac{2601}{9} = 289, \qquad N_2 = \frac{2601}{17^2} = \frac{2601}{289} = 9.$$

Obtained the linear congruences

$$N_1 x_1 = 289x_1 \equiv x_1 \equiv 1 \pmod 9,$$

$$N_2 x_2 = 9x_2 \equiv 1 \pmod{289}.$$

The solutions are $x_1 \equiv 1 \pmod 9$ and $x_2 \equiv 257 \pmod{289}$. Hence, the unique solutions of each linear congruence system are:

- Solution of linear congruence system 1

$$x \equiv 3N_1x_1 + 261N_2x_2 \equiv 3 \cdot 289 \cdot 1 + 261 \cdot 9 \cdot 257 \pmod{2601}$$
$$\equiv 867 + 603693 \equiv 604560 \equiv 1128 \pmod{2601}.$$

- Solution of linear congruence system 2

$$x \equiv 3N_1x_1 + 8N_2x_2 \equiv 3 \cdot 289 \cdot 1 + 8 \cdot 9 \cdot 257 \pmod{2601}$$
$$x \equiv 867 + 18504 \equiv 19371 \equiv 1164 \pmod{2601}.$$

- Solution of linear congruence system 3

$$x \equiv 3N_1x_1 + 169N_2x_2 \equiv 3 \cdot 289 \cdot 1 + 169 \cdot 9 \cdot 257 \pmod{2601}$$
$$\equiv 867 + 390897 \equiv 391764 \equiv 1614 \pmod{2601}.$$

So, the solutions of the polynomial congruence $f(x) = 2x^3 - 9x^2 + 17x - 6 \equiv 0 \pmod{2601}$ are $x \equiv 1128 \pmod{2601}$, $x \equiv 1164 \pmod{2601}$, and $x \equiv 1614 \pmod{2601}$.

4. CONCLUSION

Based on the research results obtained in the previous section, the conclusions of this study are as follows: first, the solution of a polynomial congruence modulo prime numbers can be determined using the recursive formula of Hensel's Lemma; second, a polynomial congruence modulo an arbitrary positive integer can be solved using Hensel's Lemma with the following steps:

1. Factorize the modulo of the polynomial congruence using the Fundamental Theorem of Arithmetic.
2. Determine the solution of the polynomial congruence for each modulo prime number.
3. Check whether the solution satisfies the conditions of Hensel's Lemma.
4. Perform the iteration process using the recursive formula of Hensel's Lemma to obtain the solution of the polynomial congruence modulo prime power.
5. Use the Chinese Remainder Theorem to combine all solutions obtained into the initial modulo solution.

Beyond these procedural steps, this hybrid algorithm offers several theoretical advantages compared to classical methods. Traditional approaches often rely on direct computation or exhaustive search, which quickly become infeasible for large moduli. In contrast, the recursive formula using Hensel's Lemma allows solutions to be built iteratively from simpler cases modulo p, avoiding recomputation at higher powers and significantly reducing computational complexity. The use of the Chinese Remainder Theorem ensures that these local solutions can be combined into a global solution efficiently. This hybrid algorithm highlights the novelty of the method. It unifies prime power lifting and modulus factorization into a systematic algorithm that scales better for large moduli.

The potential applications of this approach are promising. Recursive formula and modular solution techniques are central in computational number theory and widely used in cryptography, coding theory, and factorization problems. Future work could investigate the efficiency of the hybrid algorithm in practice, compare its complexity with other algorithms, and develop computer implementations to handle very large numbers. In addition, further theoretical exploration could address cases where the derivative condition in Hensel's Lemma fails, broadening the scope of applicability.

Author Contributions

Eka Oktaviansyah: Conceptualization, formal analysis, validation, writing - original draft. Edi Kurniadi: Conceptualization, funding acquisition, resources, supervision, validation, writing - review & editing. Dianne Amor Kusuma: Conceptualization, data curation, project administration, validation. All authors discussed the results and contributed to the final manuscript.

Funding Statement

This work was supported by the Directorate of Research and Community Service (DRPM) of Universitas Padjadjaran through the Riset Kompetensi Dosen Unpad scheme (Grant No. 4581/UN6.D/PT.00/2025).

Acknowledgment

The Authors would like to thank the reviewers for their valuable advice to improve this paper. The authors would also like to acknowledge the support received by Riset Kompetensi Dosen Unpad, the Directorate of Research and Community Service (DRPM), and the Faculty of Mathematics and Natural Sciences of Universitas Padjadjaran, Sumedang, Indonesia.

Declarations

The authors declare that there are no conflicts of interest.

REFERENCES

[1] P. S. Rudman, *HOW MATHEMATICS HAPPENED: THE FIRST 50,000 YEARS*. New York: Prometheus Books, 2007.
[2] M. Lemma and D. Allard, "APPLICATIONS OF CONGRUENCE TO DIVISIBILITY THEORY," *IJRDO-Journal Math.*, vol. 3, no. 11, pp. 32–42, 2017.
[3] G. Knapp, "POLYNOMIAL ROOT DISTRIBUTION AND ITS IMPACT ON SOLUTIONS TO THUE EQUATIONS," Ph.D. dissertation, University of Oregon, 2023.
[4] J. Bayer, M. David, B. Stock, A. Pal, Y. Matiyasevich, and D. Schleicher, "DIOPHANTINE EQUATIONS AND THE DPRM THEOREM," *Arch. Form. Proofs*, 2022.
[5] B. Grechuk, "DIOPHANTINE EQUATIONS: A SYSTEMATIC APPROACH," 2021, [Online]. Available: https://arxiv.org/abs/2108.08705
[6] O. Ikponmwosa-Eweka and A. Ozigagun, "APPLICATION OF RESPONSE SURFACE METHODOLOGY (RSM) TO PREDICT PENETRATION AREA DURING TIG WELDING AT STEADY STATE CONDITION," *NIPES - J. Sci. Technol. Res.*, vol. 5, no. 3, pp. 94 – 100, 2023.
[7] A. A. Kostoglotov, I. V Kalienko, A. S. Kornev, and S. V Lazarenko, "SYNTHESIS OF ALGORITHMS FOR COMPENSATING SYSTEMATIC ERRORS BASED ON THE CONSTRUCTION OF POLYNOMIAL MATHEMATICAL MODELS OF RADAR MEASUREMENTS," *Meas. Tech.*, vol. 65, no. 4, pp. 290 – 296, 2022. doi: https://doi.org/10.1007/s11018-022-02081-w
[8] M. Pagano, I. Tananko, and E. Stankevich, "ON THE OPTIMAL INPUT RATE IN QUEUES WITH BATCH SERVICE," *Axioms*, vol. 12, no. 7, 2023.doi: https://doi.org/10.3390/axioms12070656
[9] M. Schroeder, *NUMBER THEORY IN SCIENCE AND COMMUNICATION: WITH APPLICATIONS IN CRYPTOGRAPHY, PHYSICS, DIGITAL INFORMATION, COMPUTING, AND SELF-SIMILARITY*, 5th ed. Berlin: Springer-Verlag, 2009.
[10] A. Mosunov, "ABSOLUTE BOUND ON THE NUMBER OF SOLUTIONS OF CERTAIN DIOPHANTINE EQUATIONS OF THUE AND THUE-MAHLER TYPE," 2022, [Online]. Available: https://arxiv.org/abs/2206.13653
[11] A. Gherga and S. Siksek, "EFFICIENT RESOLUTION OF THUE-MAHLER EQUATIONS," 2022, [Online]. Available: https://arxiv.org/abs/2207.14492
[12] T. Chinburg, B. Hemenway, N. Heninger, and Z. Scherr, "CRYPTOGRAPHIC APPLICATIONS OF CAPACITY THEORY: ON THE OPTIMALITY OF COPPERSMITH'S METHOD FOR UNIVARIATE POLYNOMIALS," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10031 LNCS, pp. 759 – 788, 2016. doi: https://doi.org/10.1007/978-3-662-53887-6_28
[13] R. K. Koppanati and K. Kumar, "P-MEC: POLYNOMIAL CONGRUENCE-BASED MULTIMEDIA ENCRYPTION TECHNIQUE OVER CLOUD," *IEEE Consum. Electron. Mag.*, vol. 10, no. 5, pp. 41 – 46, 2021. doi: https://doi.org/10.1109/MCE.2020.3003127
[14] K. Bibak, B. M. Kapron, and V. Srinivasan, "AUTHENTICATION OF VARIABLE LENGTH MESSAGES IN QUANTUM KEY DISTRIBUTION," *EPJ Quantum Technol.*, vol. 9, no. 1, 2022. doi: https://doi.org/10.1140/epjqt/s40507-022-00127-0
[15] G. Ghosal, "A STUDY ON THE DEVELOPMENT AND APPLICATION OF NUMBER THEORY IN ENGINEERING FIELD," *Int. J. Inf. Sci. Comput.*, vol. 7, pp. 109–114, 2020. doi: https://doi.org/10.30954/2348-7437.2.2020.5
[16] H. H. Chan and K. Chen, "THE FUNDAMENTAL THEOREM OF ARITHMETIC AND Q-SERIES," *Math. Mag.*, vol. 97, pp. 187–193, 2024. doi: https://doi.org/10.1080/0025570X.2024.2312094
[17] I. Ahmad, B. Lee, and S. Shin, "ANALYSIS OF CHINESE REMAINDER THEOREM FOR DATA COMPRESSION," in *Proc. Int. Conf. Inf. Netw.*, Barcelona, 2020. doi: https://doi.org/10.1109/ICOIN48656.2020.9016442
[18] E. A. Alhassan *et al.*, "ON SOME ALGEBRAIC PROPERTIES OF THE CHINESE REMAINDER THEOREM WITH APPLICATIONS TO REAL LIFE," *J. Appl. Math. Comput.*, vol. 5, pp. 219–224, 2021. doi: https://doi.org/10.26855/jamc.2021.09.008
[19] I. Weiss, "SURVEY ARTICLE: THE REAL NUMBERS–A SURVEY OF CONSTRUCTIONS," *Rocky Mt. J. Math.*, vol. 45, pp. 737–762, 2015. doi: https://doi.org/10.1216/RMJ-2015-45-3-737
[20] F. Q. Gouvêa, *P-ADIC NUMBERS: AN INTRODUCTION*. Berlin: Springer, 2020. doi: https://doi.org/10.1007/978-3-030-47295-5

[21] J. Gallian, *Contemporary abstract algebra*, 10th ed. London: Chapman and Hall/CRC, 2021. doi: https://doi.org/10.1201/9781003142331
[22] K. H. Rosen, *ELEMENTARY NUMBER THEORY AND ITS APPLICATIONS*, 7th ed. London: Pearson, 2023.
[23] D. M. Burton, *ELEMENTARY NUMBER THEORY*, 7th ed. New York: McGraw-Hill, 2010.