PERKONGRUENAN POLINOMIAL MODULO m

Nunung Fajar Kusuma
Program Studi Pendidikan Matematika Pasca Sarjana Universitas Sebelas Maret
Jl. Ir. Sutami 36A Kentingan Jebres Surakarta, e-mail: nfjar@yahoo.com

Abstrak

Tujuan dari penulisan artikel ini adalah 1) Untuk mengetahui bentuk umum perkongruenan polinomial modulo m. 2) Untuk mendeskripsikan langkah-langkah penyelesaian perkongruenan polinomial modulo m dengan Hensel's Lemma. Dalam artikel ini dapat disimpulkan sebagai berikut. 1) Pengkongruenan polinomial modulo m adalah suatu perkongruenan derajat tinggi modulo m dengan derajat tertingginya n. Bentuk umum dari perkongruenan polinomial modulo m adalah sebagai berikut: $a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \equiv 0 \ (mod\ m)$. Dengan $a_n \neq 0 \ (mod\ m)$, $n > 1$ dan n bilangan bulat. 2) Penyelesaian Pengkongruenan polinomial modulo m menggunakan Hensel's Lemma. Syarat suatu Pengkongruenan polinomial modulo m dapt diselesaikan menggunakan Hensel's Lemma; a) p adalah bilangan prima. b) $f(x)$ adalah fungsi yang terdifferensialkan. Langkah-langkah penyelesaian $f(x) \equiv 0 \ (mod\ m)$: i) Perhatikan bahwa $m = p^k$, kemudian menentukan penyelesaian $f(x) \equiv 0 \ (mod\ p)$. ii) Menentukan turunan pertama untuk $f(m_1)$. iii) Menentukan invers untuk $f'(m_1) \equiv r \ (mod\ p)$. iv) Menentukan penyelesaian untuk $x \equiv m_1 \ (mod\ p)$. v) Mengulangi langkah ke iv) untuk $m_2, m_3, \ldots, m_n$.

Kata kunci: Perkongruenan, Polinomial, Modulo m.

.

1. PENDAHULUAN

a. LATAR BELAKANG

Kongruensi adalah cara lain untuk mengkaji keterbagian dalam bilangan bulat. Relasi dengan tanda " $\equiv$ " disebut relasi kongruensi. Selain kongruensi, dalam perkuliahan teori bilangan dipelajari juga tentang perkongruenan modulo m. Perkongruenan modulo m adalah kalimat terbuka yang menggunakan relasi kongruensi modulo m.

Perkongruenan modulo m terdiri dari perkongruenan linear modulo m dan perkongruenan polinomial modulo m. Perkongruenan linear modulo m adalah kalimat terbuka yang melibatkan relasi kongruensi modulo m dan variabel dari perkongruenan tersebut paling tinggi berpangkat 1. Sedangkan perkongruenan polinomial modulo m adalah suatu polinom yang melibatkan relasi kongruensi modulo m. Perkongruenan polinomial modulo m yang dipelajari dalam perkuliahan hanya perkongruenan derajat dua modulo m. Perkongruenan derajat dua modulo m adalah kalimat terbuka yang menggunakan relasi kongruensi modulo m dan variabel dari perkongruenan tersebut paling tinggi berpangkat 2.

Sifat-sifat yang berlaku dalam relasi kongruensi juga berlaku dalam perkongruenan modulo m. Perkongruenan modulo m mempunyai beberapa sifat yang sama dengan persamaan dalam Aljabar. Masalah utama persamaan dalam Aljabar adalah menentukan akar-akar suatu persamaan yang dinyatakan dalam bentuk $f(x) = 0$ dengan $f(x)$ adalah polinomial. Demikian pula halnya dengan perkongruenan polinomial modulo m,

permasalahannya adalah menentukan bilangan bulat x sehingga memenuhi $f(x) \equiv 0\ (mod\ m)$.

Penyelesaian permasalahan pada perkongruenan polinomial modulo m yang dipelajari dalam perkuliahan adalah penyelesaian dari perkongruenan derajat dua modulo m. Oleh karena itu, penulis tertarik untuk mempelajari lebih jauh perkongruenan polinomial modulo m khususnya tentang bentuk umum dan penyelesaian dari perkongruenan derajat tiga modulo m. Perkongruenan derajat tiga modulo m adalah kalimat terbuka yang menggunakan relasi kongruensi modulo m dan variabel dari perkongruenan tersebut paling tinggi berpangkat 3. Penyelesaian perkongruenan derajat tiga modulo m dengan cara biasa terlalu panjang dan rumit. Oleh karena itu, penulis ingin membahas penyelesain lain yaitu penyelesain dengan Hensel's Lemma.

Untuk lebih memberikan gambaran bagaimana perbedaan penyelesaian tersebut pada artikel ini akan dibahas penyelesaian dari perkongruenan derajat tiga modulo m dengan cara biasa dan dengan Hensel's Lemma. Tujuan dari penulisan makalah ini adalah 1) Untuk mengetahui bentuk umum perkongruenan polinomial modulo m. 2) Untuk mendeskripsikan langkah-langkah penyelesaian perkongruenan polinomial modulo m dengan Hensel's Lemma.

b. KAJIAN TEORI

1) Kekongruenan Modulo m

Definisi

Bila dua bilangan bulat a dan b dibagi dengan bilangan bulat positif (bilangan asli) m dan mempunyai sisa sama maka dikatakan bahwa a kongruen dengan b modulo m, dan ditulis $a \equiv b(mod\ m)$.

Demikian juga bila b kongruen dengan a modulo m dapat ditulis: $b \equiv a(mod\ m)$

$$a \equiv b(mod\ m)$$
$$a - b = km \leftrightarrow m \mid a - b,$$

dengan k adalah bilangan bulat.

Sehingga $(b - a) = (-k)m \leftrightarrow m \mid b - a$

Jadi, bila $a \equiv b(mod\ m)$, maka juga berlaku $b \equiv a(mod\ m)$.

(Purwoto, 2000: 89)

2) Polinomial

Polinomial adalah suku banyak berderajat n, dengan n bilangan cacah.

Bentuk umum: $a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2 x^2 + a_1 x + a_0$.

$a_n \neq 0, a_n, a_{n-1}, \ldots, a_2, a_1$ dinamakan koefisien, $x^n, x^{n-1}, x^{n-2}, \ldots, x^2, x$ dinamakan variabel berpangkat, $n, n-1, n-2, \ldots, 2, 1$ dinamakan pangkat dan a_0 dinamakan suku tetap.

Dengan $a_n, a_{n-1}, \ldots, a_2, a_1$ adalah bilangan bulat.

Untuk memudahkan cara menyebutnya polinomial dinyatakan dengan $f(x)$.

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2 x^2 + a_1 x + a_0$$

(Pargiyo, 2002:45)

3) Perkongruenan Linear Modulo m

Perkongruenan adalah kalimat terbuka yang menggunakan relasi kongruensi. Suatu perkongruean $ax^n \equiv b\ (mod\ m)$, dengan $n = 1$ disebut perkongruenan linear.

Bentuk umum:

$ax \equiv b(mod\ m)$, dengan $a \neq 0$.

Telah diketahui bahwa $ax \equiv b(mod\ m)$ berarti $ax - b = k.m$ atau $ax = b + k.m$, maka perkongruenan linear $ax \equiv b(mod\ m)$ akan mempunyai solusi (penyelesaian) bila dan hanya bila ada bilangan-bilangan bulat x dan k yang memenuhi persamaan $ax = b + k.m$.

(Purwoto, 2000:119)

4) Perkongruenan Derajat Dua Modulo m

Perkongruenan Derajat Dua modulo m adalah kalimat terbuka yang menggunakan relasi kongruensi modulo m dan variabel dari perkongruenan tersebut paling tinggi berpangkat 2. Bentuk umum dari perkongruenan derajat dua modulo m adalah sebagai berikut:

$$a_2x^2 + a_1x + a_0 \equiv 0(mod\ m)$$

Dengan a_2, a_1, a_0 dan m bilangan-bilangan bulat, $a_2 \not\equiv 0(mod\ m)$.

Perkongruenan derajat dua modulo m adalah suatu perkongruenan derajat tinggi modulo m dengan derajat tertingginya adalah 2. Oleh karena itu, sifat-sifat yang dipenuhi untuk perkongruenan derajat tinggi (polinom) modulo m dipenuhi pula untuk perkongruenan derajat dua modulo m.

(Purwoto, 2000:134)

5) Perkongruenan Derajat Tiga modulo m

Perkongruenan Derajat Tiga modulo m adalah kalimat terbuka yang menggunakan relasi kongruensi modulo m dan variabel dari perkongruenan tersebut paling tinggi berpangkat 3. Bentuk umum dari perkongruenan derajat tiga modulo m adalah sebagai berikut:

$$a_3x^3 + a_2x^2 + a_1x + a_0 \equiv 0(mod\ m)$$

Dengan a_3, a_2, a_1, a_0 dan m bilangan-bilangan bulat, $a_3 \not\equiv 0(mod\ m)$.

Perkongruenan derajat tiga modulo m adalah suatu perkongruenan derajat tinggi modulo m dengan derajat tertingginya adalah 3. Oleh karena itu, sifat-sifat yang dipenuhi untuk perkongruenan derajat tinggi (polinom) modulo m dipenuhi pula untuk perkongruenan derajat tiga modulo m.

Pada perkongruenan derajat tinggi (polinom) modulo m jika terdapat a suatu residu modulo m sehingga $f_1(a) \equiv f_2(a)(mod\ m)$ maka dikatakan a solusi dari perkongruenan tersebut.

(Bana Kartasasmita, 1982: 61)

6) Hensel's Lemma

Teorema

Andaikan $f(x)$ suatu polinomial dengan koefisien bilangan bulat, p suatu bilangan prima, dan a merupakan solusi untuk kongruensi $f(x) \equiv 0\ (mod\ p^j)$ sehingga $f'(x) \not\equiv 0\ mod\ p$. Maka ada sebuah bilangan bulat t sehingga $a + tp^j$ merupakan solusi untuk kongruensi $f(x) \equiv 0\ (mod\ p^{j+1})$.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian studi literatur. Metodologi yang digunakan adalah mengumpulkan bahan tulisan dari buku-buku dan jurnal maupun makalah yang membahas perkongruenan polinomial modulo m. Artikel memberikan gambaran bagaimana perbedaan penyelesaian perkongruenan polinomial modulo m pada makalah ini akan dibahas penyelesaian dari perkongruenan derajat tiga modulo m dengan cara biasa dan dengan Hensel's Lemma. Tujuan dari penulisan makalah ini adalah 1) Untuk mengetahui bentuk umum perkongruenan polinomial modulo m. 2) Untuk mendeskripsikan langkah-langkah penyelesaian perkongruenan polinomial modulo m dengan Hensel's Lemma.

3. HASIL PENELITIAN DAN PEMBAHASAN

a. Bentuk Umum Perkongruenan Polinomial Modulo m

Perkongruenan polinomial modulo m adalah suatu perkongruenan derajat tinggi modulo m dengan derajat tetingginya n. Bentuk umum dari perkongruenan polinomial modulo m adalah sebagai berikut:

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \equiv 0\ (mod\ m)$$

Dengan $a_n \not\equiv 0\ (mod\ m)$, $n \geq 1$ dan n bilangan bulat

Teorema 1

Andaikan f suatu polinom dengan koefisien bilangan bulat, yaitu:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

Dengan $a_{n,}a_{n-1,}a_{n-2,} \ldots, a_0$ masing-masing bilangan bulat. Jika $a \equiv b(mod\ m)$ maka $f(a) \equiv f(b)(mod\ m)$.

Bukti Teorema 1

Karena $a \equiv b(mod\ m)$ maka $a^n \equiv b^n(mod\ m)$, berdasarkan Teorema 7.

Berarti $a_n a^n \equiv a_n b^n(mod\ m)$, $a_{n-1}a^{n-1} \equiv a_{n-1}b^{n-1}(mod\ m)$ dan seterusnya menurut pangkatnya hingga $a_1 a \equiv a_1 b(mod\ m)$, sedangkan $a_0 \equiv a_0(mod\ m)$.

Dengan menggunakan Teorema 3, dapat diperoleh:

$a_n a^n + a_{n-1}a^{n-1} + \cdots + a_1 a + a_0$

$\equiv a_n b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 (mod\ m)$

Atau $f(a) \equiv f(b)(mod\ m)$.

Jadi, terbukti jika a adalah solusi polinom $f(x)$ dengan koefisien bilangan bulat sedangkan $a \equiv b(mod\ m)$. Maka b menjadi solusi $f(x)$ untuk modulo m.

(Terbukti)

Teorema 2

Jika $x \equiv r(mod\ m)$ merupakan solusi perkongruenan $f(x) \equiv 0(mod\ m)$ dengan

$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0; a_{n,} a_{n-1,} a_{n-2,} \ldots, a_0$ bilangan bulat dan $a_n \equiv 0(mod\ m)$, maka $(x - r)$ adalah faktor dari $f(x)(mod\ m)$ dan sebaliknya.

Bukti Teorema 2

Menurut Teorema Sisa Aljabar, $f(r)$ adalah sisa apabila $f(x)$ dibagi $(x - r)$.

$$f(x) = q(x)(x - r) + f(r)$$

atau $f(x) - f(r) = q(x)(x - r)$

dan $q(x) = b_0 x^{n-1} + b_1 x^{n-2} + bx^{n-3} + \cdots + b_{n-2}x^1 + b_{n-1}x^0$

dengan $b_{0,} b_{1,} b_{2,} \ldots, b_{n-1}$ bilangan bulat.

Sehingga

$$f(x) - f(r) \equiv (x - r)q(x)(mod\ m)$$

dan $f(x) \equiv (x - r)q(x)(mod\ m)$

karena $f(r) \equiv 0(mod\ m)$

Ini berarti $(x - r)$ merupakan faktor modulo m untuk $f(x)$.

Andaikan sebaliknya, maka:

$f(x) - f(r) \equiv (x - r)q(x)(mod\ m)$ sehingga

$f(r) \equiv (r - r)q(x)(mod\ m)$

$f(r) \equiv 0(mod\ m)$

Ini artinya $x \equiv r(mod\ m)$ solusi dari $f(r) \equiv 0(mod\ m)$.

(Terbukti)

b. Penyelesaian Perkongruenan Derajat Tiga Modulo m

Penyelesaian Perkongruenan derajat tiga modulo m ada berbagai cara antara lain adalah sebagai berikut:

1) Cara Biasa

Cara ini disebut biasa karena kita hanya membuat barisan bilangan yang memenuhi masing-masing kongruensi, dan dilanjutkan dengan pencarian unsur persekutuan dari semua kongruensi. Penetapan penyelesaian didasarkan pada teorema kekongruenan.

Langkah-langkah Penyelesaian $a_3 x^3 + a_2 x^2 + a_1 x + a_0 \equiv 0(mod\ m)$:

a) Mencari perkalian dua bilangan yang memenuhi m. Misal dua bilangan itu adalah m_1 dan m_2.

Dengan m_1 dan m_2 adalah bilangan bulat.

Atau ditulis: $m = m_1 \times m_2$

b) Memecah kongruensi menjadi dua bagian, yaitu:
$a_3x^3 + a_2x^2 + a_1x + a_0 \equiv 0(mod\ m_1) \dots (i)$
$a_3x^3 + a_2x^2 + a_1x + a_0 \equiv 0(mod\ m_2) \dots (ii)$

c) Mencari solusi untuk (i) dan (ii).

i. Jika m_1 atau m_2 adalah bilangan tertentu berpangkat k maka dicari terlebih dahulu solusi untuk bilangan itu.
Misal: $m_1 = p^k$,
dengan p adalah bilangan prima.
$k \geq 2$ dan k adalah bilangan bulat.
Ditulis:
$a_3x^3 + a_2x^2 + a_1x + a_0 \equiv 0(mod\ p) \dots (iii)$
$a_3x^3 + a_2x^2 + a_1x + a_0 \equiv 0(mod\ p^k) \dots (iv)$

Mencari solusi untuk $a_3x^3 + a_2x^2 + a_1x + a_0 \equiv 0(mod\ p)$.
Langkah-langkahnya:

- Menggunakan cara coba-coba dengan memasukkan $x = 0,1,2,3,4, \dots, (p-1)$ yang memenuhi kongruensi tersebut.
  Misal: q memenuhi persamaan itu.
  Diperoleh,
  $a_3q^3 + a_2q^2 + a_1q + a_0 \equiv 0(mod\ p)$
  Sehingga solusinya adalah $x \equiv q\ (mod\ p)$
  atau $x = pt + q$ dimana t adalah bilangan bulat.
- Mensubtitusikan $x = pt + q$ ke (iv), sehingga diperoleh:
$$a_3x^3 + a_2x^2 + a_1x + a_0 \equiv 0(mod\ p^k)$$
$$\leftrightarrow (a_3p^{3)})t^3 + (a_3p^2q + 2a_3p^2q + a_2p^2)t^2 + (2a_3pq^2 + a_3pq^2 + 2a_2pq + a_1p)t + (a_3q^3 + a_2q^2 + a_1q + a_0) \equiv 0(mod\ p^k)$$
- Membuat
  $(a_3p^{3)})t^3 + (a_3p^2q + 2a_3p^2q + a_2p^2)t^2 + (2a_3pq^2 + a_3pq^2 + 2a_2pq + a_1p)t + (a_3q^3 + a_2q^2 + a_1q + a_0) \equiv 0(mod\ p^k)$
  menjadi bentuk linear.
  Berapapun nilai
  $t, (a_3p^3)t^3 + (a_3p^2q + 2a_3p^2q + a_2p^2)t^2$ selalu habis dibagi p^k.
  Oleh karena itu dapat dihilangkan. Sehingga menjadi:
  $(a_3p^{3)}\cancel{t^3} + \cancel{(a_3p^2q + 2a_3p^2q + a_2p^2)}t^2 + (2a_3pq^2 + a_3pq^2 + 2a_2pq + a_1p)t + (a_3q^3 + a_2q^2 + a_1q + a_0) \equiv 0(mod\ p^k)$
  $(2a_3pq^2 + a_3pq^2 + 2a_2pq + a_1p)t + (a_3q^3 + a_2q^2 + a_1q + a_0) \equiv 0(mod\ p^k)$
- Membagi kedua ruas dengan p.
$$\frac{(2a_3pq^2 + a_3pq^2 + 2a_2pq + a_1p)}{p}t + \frac{(a_3q^3 + a_2q^2 + a_1q + a_0)}{p} \equiv 0\left(mod\ \frac{p^k}{FPB(p, p^k)}\right)$$

$\leftrightarrow rt + s \equiv 0(mod\ p^{k-1})$,
dengan $r = \frac{(2a_3pq^2+a_3pq^2+2a_2pq+a_1p)}{p}$ dan $s = \frac{(a_3q^3+a_2q^2+a_1q+a_0)}{p}$.

Berapapun nilai r dan s selalu habis dibagi p^{k-1}. Sehingga r dan s juga selalu habis dibagi p. Oleh karena itu perkongruenannya menjadi:

$\leftrightarrow rt + s \equiv 0(mod\ p)$
$\leftrightarrow rt \equiv -s(mod\ p)$
$\leftrightarrow rt \equiv p - s(mod\ p)$
$\leftrightarrow rt \equiv u\ (mod\ p)$
$\leftrightarrow t \equiv v(mod\ p)$

Maka kita peroleh solusinya sebagai berikut:

$$x = pt + q = p(pk + v) + q = p^2k + (pv + q)$$
$$x \equiv (pv + q)\ (mod\ p^2)$$

Jika m_1 atau m_2 adalah bilangan tertentu berpangkat k maka solusinya dicari dengan menggunakan cara coba-coba dengan memasukkan
$x = 0,1,2,3,4, \dots, (p-1)$ yang memenuhi kongruensi tersebut.

Misal: y memenuhi persamaan itu.
Diperoleh,
$a_3q^3 + a_2q^2 + a_1q + a_0 \equiv 0(mod\ m_1)$ atau
$a_3q^3 + a_2q^2 + a_1q + a_0 \equiv 0(mod\ m_2)$.
Sehingga solusinya adalah $x \equiv y\ (mod\ m_2)$.
atau $x = m_2l + y$ dimana l adalah bilangan bulat.

Mencari penyelesaian untuk kedua solusi yang telah ditemukan.

i. $x \equiv (pv + q)\ (mod\ p^2) \rightarrow x = p^2k + (pv + q)$
ii. $x \equiv q\ (mod\ m_2) \rightarrow x = m_2l + y$

$$p^2k + (pv + q) = m_2l + y$$
$$p^2k = m_2l + (pv + q + y)$$

Invers dari p^2 modulo m_2 adalah $-z$.
Diperoleh dari $1 = m_2 + p^2(-z)$.

$$p^2k \equiv (pv + q + y)\ (mod\ m_2)$$
$$k \equiv (-z)(pv + q + y)\ (mod\ m_2)$$
$$k \equiv w\ (mod\ m_2)$$
$$k = m_2n + w$$

Mensubtitusikan nilai $k = m_2n + w$ ke $x = p^2k + (upv + q)$.
Sehingga diperoleh:
$x = p^2(m_2n + w) + (pv + q) = p^2m_2n + (p^2w + pv + q)$
$x \equiv (p^2w + pv + q)(mod\ p^2m_2)$.

2) Hensel's Lemma

Langkah-langkah penyelesaian $f(x) \equiv 0 \ (mod\ m)$:

a) Perhatikan bahwa $m = p^k$, kemudian menentukan penyelesaian $f(x) \equiv 0 \ (mod\ p)$, dimana $f(x)$ adalah fungsi yang terdifferensialkan.
   Dimana $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$
   m adalah bilangan bulat
   p adalah bilangan prima.
   $k \geq 2$ dan k adalah bilangan bulat.
   Misalkan akar-akar tersebut adalah $m_1, m_2, m_3, \dots, m_n$.

b) Menentukan turunan pertama untuk $f(m_1)$.
   $f'(m_1) = 3a_3{m_1}^2 + 2a_2m_1 + a_1$

c) Menentukan invers untuk $f'(m_1) \equiv 3a_3{m_1}^2 + 2a_2m_1 + a_1 \ (mod\ p)$.
   $f'(m_1)^{-1} = q \times 3a_3{m_1}^2 + 2a_2m_1 + a_1 \equiv 1 \ (mod\ p)$.
   Dengan q adalah suatu bilangan bulat.

d) Menentukan penyelesaian untuk $x \equiv m_1 \ (mod\ p)$.
   $b_1 \equiv m_1 \ (mod\ p)$
   $b_2 \equiv (a_1 - f(a_1)f'(m_1)^{-1}) \ (mod\ p^2)$
   $b_3 \equiv (a_2 - f(a_2)f'(m_1)^{-1}) \ (mod\ p^3)$
   $\vdots$
   $b_n \equiv \left(a_{n-1} - f(a_{n-1})f'(m_1)^{-1}\right) (mod\ p^n)$

e) Mengulangi langkah ke 4) untuk $m_2, m_3, \dots, m_n$.

Langkah-langkah penyelesaian $f(x) \equiv 0 \ (mod\ m)$:

a) Perhatikan bahwa $m = p^k$, kemudian menentukan penyelesaian $f(x) \equiv 0 \ (mod\ p)$, dimana $f(x)$ adalah fungsi yang terdifferensialkan.
   Dimana $f(x) = a_2x^2 + a_1x + a_0$
   m adalah bilangan bulat.
   p adalah bilangan prima.
   $k \geq 2$ dan k adalah bilangan bulat.
   Misalkan akar-akar tersebut adalah $m_1, m_2, m_3, \dots, m_n$.

b) Menentukan turunan pertama untuk $f(m_1)$.
   $f'(m_1) = 2a_2m_1 + a_1$

c) Menentukan invers untuk $f'(m_1) \equiv 2a_2m_1 + a_1 \ (mod\ p)$.
   $f'(m_1)^{-1} = q \times (2a_2m_1 + a_1) \equiv 1 \ (mod\ p)$.
   Dengan q adalah suatu bilangan bulat.

d) Menentukan penyelesaian untuk $x \equiv m_1 \ (mod\ p)$.

$b_1 \equiv m_1 \ (mod\ p)$

$b_2 \equiv (a_1 - f(a_1)f'(m_1)^{-1}) \ (mod\ p^2)$

$b_3 \equiv (a_2 - f(a_2)f'(m_1)^{-1}) \ (mod\ p^3)$

$\vdots$

$b_n \equiv \left(a_{n-1} - f(a_{n-1})f'(m_1)^{-1}\right) (mod\ p^n)$

e) Mengulangi langkah ke 4) untuk $m_2, m_3, \dots, m_n$.

4. SIMPULAN

Berdasarkan pembahasan maka dapat diambil beberapa kesimpulan yaitu:

1. Pengkongruenan polinomial modulo m adalah suatu perkongruenan derajat tinggi modulo m dengan derajat tertingginya n. Bentuk umum dari perkongruenan polinomial modulo m adalah sebagai berikut:

   $$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \equiv 0 \ (mod\ m)$$

   Dengan $a_n \neq 0 \ (mod\ m)$, $n > 1$ dan n bilangan bulat
2. Penyelesaian Pengkongruenan polinomial modulo m menggunakan Hensel's Lemma.

   Syarat suatu Pengkongruenan polinomial modulo m dapt diselesaikan menggunakan Hensel's Lemma:

   a) p adalah bilangan prima
   b) $f(x)$ adalah fungsi yang terdifferensialkan.

   Langkah-langkah penyelesaian $f(x) \equiv 0 \ (mod\ m)$:

   1) Perhatikan bahwa $m = p^k$, kemudian menentukan penyelesaian $f(x) \equiv 0 \ (mod\ p)$.
   2) Menentukan turunan pertama untuk $f(m_1)$. Misalkan $f'(m_1) = r$.
   3) Menentukan invers untuk $f'(m_1) \equiv r \ (mod\ p)$.
   4) Menentukan penyelesaian untuk $x \equiv m_1 \ (mod\ p)$.
   5) Mengulangi langkah ke 4) untuk $m_2, m_3, \dots, m_n$.

5. DAFTAR PUSTAKA

Anonim. (2013). *Deret Taylor*. Diakses dari http://id.wikipedia.org/wiki/Deret_Taylor.

Bana Kartasasmita. (1982). *Pengantar Teori Bilangan*. Bandung: ITB.

Hendry dext. (2009). *Kongruensi Polinomial dan Hensel Lemma*. Diakses dari http://hendrydext.blogspot.com.

Herry Sukarman. (1993). *Teori Bilangan*. Jakarta: Universitas Terbuka

Depdikbud.

Mcivor, James. (2012). *Math 115*. Lecture 10.

Pargiyo. (2002). *Aljabar*. Surakarta: Sebelas Maret University Press.

Purcell, Edwin J dan Varberg, Dale. (1987). *Kalkulus dan Geometri Anaitis Jilid I*. Jakarta: Erlangga.

Purwoto. (2000). *Teori Bilangan*. Surakarta: Sebelas Maret University Press.

Riski Yulita Sayid Putri. (2009). Pengkongruenan Derajat Dua Modulo m. Surakarta: Jurusan Matematika FKIP UNS.

Sukirman. (2006). *Pengantar Teori Bilangan.*Yogyakarta: Hanggar Kreator.