BAB IV
TEORI KONGRUENSI

4.1 Sifat Dasar Kongruensi

Definisi 4.1. Misalkan n suatu bilangan bulat positif. Dua bilangan bulat a dan b dikatakan kongruen modulo n ditulis $a \equiv b \pmod{n}$ jika n habis membagi a – b, yaitu a- b = kn untuk suatu k bilangan bulat.

Sebagi contoh untuk n = 7, definisi di atas biasa digunakan untuk memeriksa kebenaran pernyataan pernyataan $3 \equiv 24 \pmod 7$, $-31 \equiv 11 \pmod 7$, $-15 \equiv -64 \pmod 7$. Pernyataan-pernyataan itu benar sebab 3 –24 = (-3)7, -31- 11 = (-6)7 dan –15 – (-64) = 7.7. Ketika n tidak habis membagi (a-b) kita katakan a tidak kongruen dengan b modulo n, bila demikian ditulis $a \equiv b \pmod{n}$. Sebagai contoh $25 \equiv 12 \pmod 7$ karena 7 tidak habis membagi 25 – 12.

Perlu dicatat bahwa sembarang dua bilangan bulat selalu kongruen modulo 1, sedangkan dua bilangan bulat kongruen modulo 2 jika keduanya bilangan ganjil atau keduanya bilangan genap. Dengan demikian modulo 1 tidak menarik untuk dibicarakan, selanjutnya diasumsikan n > 1.

Diberikan bilangan bulat a, misalkan q dan r adalah hasil bagi dan sisa pembagian a oleh n sehingga a = qn + r, $0 \le r \le n$. Berdasarkan definisi kongruensi $a \equiv r \pmod{n}$. Karena ada n pilihan untuk r, kita ketahui bahwa setiap bilangan bulat adalah kongruen modulo n dengan satu di antara bilangan 0, 1, 2, …, n-1; khususnya $a \equiv 0 \pmod{n}$ jika dan hanya jika $n \mid a$. Himpunan n bilangan bulat 0, 1, 2, …, n –1 disebut himpunan residu positif terkecil modulo n.

Secara umum, suatu kumpulan n bilangan bulat $a_1, a_2, \ldots, a_n$ dikatakan membentuk himpunan residu lengkap modulo n jika setiap bilangan bulat tersebut kongruen modulo n dengan tepat satu a_k. Sebagai contoh –12, -4, 11, 13, 22, 82, 91 membentuk suatu residu lengkap modulo 7, karena $-12 \equiv 2$, $-4 \equiv 3$, $11 \equiv 4$, $13 \equiv 6$, $22 \equiv 1$, $82 \equiv 5$, $91 \equiv 0$ modulo 7. Dari observasi ini dapat disimpulkan bahwa n bilangan bulat membentuk himpunan residu lengkap modulo n jika dan hanya jika tidak ada dua bilangan di antara bilangan tersebut yang kongruen modulo n.

Teorema 4.1

Untuk sembarang bilangan bulat a dan b $a \equiv b$ (modulo n) jika dan hanya jika a dan b memiliki sisa positif yang sama ketika dibagi oleh n.

Bukti:

Misalkan $a \equiv b \pmod{n}$, sehingga a = b + kn untuk k suatu bilangan bulat, pembagian b oleh n, diperoleh sisa r dengan b = qn + r dengan $0 \le r < n$. Selanjutnya diperoleh a=b+kn = (qn + r) + kn = (q +k)n + r. Ini menunjukkan bahwa a dan b memiliki sisa yang sama bila dibagi oleh n.

Sebaliknya, misalkan a dan b memiliki sisa yang sama jika dibagi oleh n, yaitu $a = q_1n + r$ dan $b = q_2n + r$. dengan $0 \le r < n$. Dengan demikian $a - b = (q_1n + r) - (q_2n + r) = (q_1 - q_2)n$ atau $n \mid a - b$ atau $a \equiv b \pmod{n}$.

Contoh 4.1.

Karena –56 dan –11 dapat dinyatakan dalam bentuk –56 = (-7)9 + 7, -11 = (-2)9 + 7 dengan sisa yang sama 7, menurut teorema 4.1., –56 ≡ -11 (mod 9). Sebaliknya jika –31 ≡ 11 (mod 7), maka –31 dan 11 memiliki sisa positif yang sama ketika dibagi 7;jelasnya adalah –31 = (-5)7 + 4, 11 = 1.7 + 4.

Teorema 4.2.

Misalkan n > 1 tertentu, a, b, c, d sembarang bilangan bulat, maka pernyataan-pernyataan dibawah ini benar.

(a) a ≡ a (mod n)
(b) Jika a ≡ b (mod n), maka b ≡ a (mod n)
(c) Jika a ≡ b (mod n) dan b ≡ c (mod n), maka a ≡ c (mod n).
(d) Jika a ≡ b (mod n) dan c ≡ d (mod n), maka a+c ≡ b + d (mod n) dan ac ≡ bd (mod n).
(e) Jika a ≡ b (mod n), maka a + c ≡ b + c (mod n) dan ac ≡ bc (mod n).
(f) Jika a ≡ b (mod n), maka $a^k \equiv b^k$ (mod n) untuk sembarang k bilangan bulat.

Bukti:

(a) Untuk sembarang bilangan bulat a, maka a – a = 0.n, sehingga a ≡ a (mod n).
(b) Jika a ≡ b (mod n) maka a – b = kn untuk suatuk bilangan bulat. Sedangkan b – a = -kn = (-k)n dimana –k adalah suatu bilangan bulat, sehingga b ≡ a (mod n).
(c) Jika a ≡ b (mod n) dan b ≡ c (mod n), artinya a – b = hn dan b – c = kn, dengan demikian a – c = (a –b) + (b – c) = hn + kn = (h+k)n sehingga a ≡ c (mod n).
(d) Jika a ≡ b (mod n) dan c ≡ d (mod n), artinya a – b = hn dan c – d = kn. Dengan demikian a – c = (a –b) + (b – c) = hn + kn = (h+k)n sehingga a ≡ c (mod n). Dengan demikian (a + c) – (b+d) = (a –b) + (c – d) = hn + kn = (h + k) n atau a + c ≡ b+d (mod n). Sedangkan ac = (b + hn)(d + kn) = bd + (bh +dk + hkn) n dengan (bh + dk + hkn) suatu bilangan bulat, dengan kata lain ac – bd habis dibagi oleh n atau ac ≡ bd (mod n).
(e) Buktinya sudah tercakup dalam bukti d
(f) Bukti bagian ini menggunakan induksi matematika, untuk k = 1 benar, karena diketahui a ≡ b (mod n). Misalkan untuk k = n benar artinya $a^n \equiv b^n$ (mod n) benar. Akan ditunjukkan untuk k = n +1 benarBerdasarkan teorema (d) maka $a\, a^n \equiv b b^n$ (mod n) atau $a^{n+1} \equiv b^{n+1}$ (mod n). Dengan demikian pernyataan tersebut benar untuk semua bilangan bulat positif k.

Contoh 4.2.

Buktikan 41 membagi $2^{20} – 1$

Bukti:

Kita mulai bahwa $2^5 \equiv -9$ (mod 41), selanjutnya berdasarkan teorema 4.2.(f) $(2^5)^4 \equiv (-9)^4$ (mod 41). Dengan kata lain $2^{20} \equiv 81.81$ (mod 41), sedangkan 81 ≡ -1 (mod 41), sehingga 81.81 $\equiv$ 1 (mod 41). Dengan menggunakan teorema 4.2. (b) dan (e) 2^{20} - 1$\equiv$ 81.81 – 1 $\equiv$ 1 - 1 $\equiv$ 0 (mod 41). Jadi 41 $\mid 2^{20} - 1$.

Contoh 4.3.
Tentukan sisa pembagian 1! + 2! + 3! + 4! + … + 99! + 100! oleh 12.
Jawab:
Kita mulai dari kenyataan bahwa 4! $\equiv$ 24 $\equiv$ 0 (mod 12).
Jadi untuk $k \geq 4$ $k! \equiv 4!\,.\,5.\,6\ldots.\,k \equiv 0.5.6\ldots.k \equiv 0 \pmod{12}$.
Dengan demikian 1! + 2! + 3! + 4! + … + 100! $\equiv$ 1! + 2! + 3! + 0 + … + 0 $\equiv$ 9 (mod 12). Jadi sisa pembagian 1! + 2! + 3! + 4! + … + 100! Oleh 12 adalah 9.

Pada teorema 4.2., jika Jika $a \equiv b \pmod{n}$, maka $ac \equiv bc \pmod{n}$ untuk sembarang bilangan bulat c, tetapi pernyataan sebaliknya tidak (selalu) benar. Sebagi contoh, 2.4 $\equiv$ 2.1 (mod 6) tetapi 4 $\neq$ 1 (mod 6)

Teorema 4.3.
Jika $ca \equiv cb \pmod{n}$ dan $d = \gcd(c,n)$, maka $a \equiv b \pmod{n/d}$.
Bukti
Diketahui $ca \equiv cb \pmod{n}$ artinya $c(a - b) = ca - cb = kn$ untuk suatu bilangan bulat k. Diketahui pula $d = \gcd(c,n)$, ada bilangan bulat r dan s yang relatif prima yang memenuhi $c = dr$ dan $n = ds$, sehingga $c(a\text{-}b) = kn \Leftrightarrow r(a - b) = ks$. Karena $s \mid r\,(a - b)$ dan $\gcd(r,s) = 1$, maka menurut lemma Euclid $s \mid a - b$, dengan kata lain $a \equiv b$ (mod s) atau $a \equiv b \pmod{n/d}$.

Bukti:
Karena p prima dan p tidak membagi c, maka gcd (p,c) = 1, sehingga berlaku Akibat 1.
Jika $ca \equiv cb \pmod{n}$ dan $\gcd(c,n) = 1$ maka $a \equiv b \pmod{n}$

Akibat 1
Jika $ca \equiv cb \pmod{n}$ dan $\gcd(c,n) = 1$, maka $a \equiv b \pmod{n}$.

Akibat 2
Jika $ca \equiv cb \pmod{p}$ dan p adalah prima, $p \mid c$, maka $a \equiv b \pmod{p}$.

Contoh 4.4.
Tinjau 33 $\equiv$ 15 (mod 9) atau 3.11 $\equiv$ 3. 5 (mod 9) dan gcd(3,9) = 3. Berdasarkan teorema 4., disimpulkan 11 $\equiv$5 (mod 3).
Ilustrasi lain misal –35 $\equiv$ 45 (mod 8) atau 5 (-7) $\equiv$ 5.9 (mod 8). Bilangan 5 dan 8 relatif prima, sehingga –7 $\equiv$ 9 (mod 8).

Pada teorema 4.3., tidak perlu $c \not\equiv 0 \pmod{n}$. Jika $c \equiv 0 \pmod{n}$ maka gcd (c,n) = n, sehingga teorema tersebut menyimpulkan $a \equiv b \pmod{1}$. Berdasarkan penjelasan sebelumnya hal itu adalah sesuatu yang trivial, karena sembarang dua bilangan bulat selalu kongruen untuk modulo 1.

Dalam kongruensi jika perkalian dua bilangan bulat hasilnya 0, maka mungkin kedua duanya tidak 0. Sebagai contoh $4.3 \equiv 0 \pmod{12}$ sementara $4 \not\equiv 0 \pmod{12}$ dan $3 \not\equiv 0 \pmod{12}$. Jika $ab \equiv 0 \pmod{n}$ dan gcd(a,n) = 1, maka $b \equiv 0 \pmod{n}$ dan ini benar berdasarkan Akibat 1 $ab \equiv 0 \equiv a.0 \pmod{n}$ jika gcd (a,n) = 1, maka $b \equiv 0 \pmod{n}$. Variasi lainnya adalah jika $ab \equiv 0 \pmod{p}$ dengan p bilangan prima, maka $a \equiv 0 \pmod{p}$ atau $b \equiv 0 \pmod{p}$.

Soal-soal 4.2

1.Buktikan setiap pernyataan berikut.

(a) Jika $a \equiv b \pmod{n}$ dan $m \mid n$, maka $a \equiv b \pmod{m}$.

(b) Jika $a \equiv b \pmod{n}$ dan $c > 0$, maka $ca \equiv cb \pmod{cn}$.

(c) Jika $a \equiv b \pmod{n}$ dan a, b, n habis dibagi $d > 0$, maka $a/d \equiv b/d \pmod{n/d}$.

2. Berikan sebuah contoh utnuk menunjukkan jika $a^2 \equiv b^2 \pmod{n}$ tidak (selalu) mengakibatkan $a \equiv b \pmod{n}$.

3. Jika $a \equiv b \pmod{n}$, buktikan bahwa gcd(a,n) = gcd (b,n).

4. (a) Tentukan sisa masing-masing pembagia 2^{50} dan 41^{65} jika dibagi 7.

(b) Tentukan sisa pembagian $1^5 + 2^5 + 3^5 + \ldots 99^5 + 100^5$ oleh 4.

5. Buktikan pernyataan berikut ini

(a) Jika a bilangan ganjil maka $a^2 \equiv 1 \pmod{8}$

(b) Untuk sembarang bilangan bulat a, $a^3 \equiv 0, 1,$ atau $6 \pmod{7}$.

(c) Untuk sembarang bilangan bulat a, $a^4 \equiv 0$ atau $1 \pmod{5}$.

(d) Jika a bilangan bulat tidak habis dibagi oleh 2 atau 3, maka $a2 \equiv 1 \pmod{24}$.