II. TINJAUAN PUSTAKA

Pada bab ini akan dibahas konsep-konsep yang mendasari konsep representasi penjumlahan dua bilangan kuadrat sempurna. Seperti, teori keterbagian bilangan bulat, bilangan prima, kongruensi dalam bilangan bulat.

2.1 Keterbagian Dalam Bilangan Bulat

Definisi 2.1.1

Suatu bilangan bulat a dikatakan habis dibagi oleh suatu bilangan bulat $b \neq 0$, jika terdapat suatu bilangan bulat x sedemikin sehingga $a = bx$. Jika jal ini dipenuhi maka b dikatakan membagi a dan dinotasikan dengan $b \mid a$ yang dapat diartikan sebagai b adalah faktor (pembagi) a, atau a adalah kelipatan b. Jika b tidak habis membagi a, maka dinotasikan $b \nmid a$ (Burton, 1998).

Teorema 2.1.2 (Algoritma Pembagian)

Jika $a > 0$, dan $a, b \in \mathbb{Z}$, maka ada bilangan-bilangan $q, r \in \mathbb{Z}$ yang masing-masing tunggal (unique), sehingga $b = qa + r$ dengan $0 \leq r < a$. jika $a \nmid b$ maka r memenuhi ketidaksamaan $0 < r < a$.

b disebut bilangan yang dibagi (*devided*)

a disebut bilangan pembagi (*devisor*/pembagi)

q disebut bilangan hasil (*quotient*), dan

r disebut bilangan sisa (*remaider*/residu)

Sifat- sifat keterbagian bilangan bulat

1. $a \mid 0, 1 \mid a, a \mid a.$
2. $a \mid 1$, jika dan hanya jika $a = \pm 1.$
3. Jika $a \mid b$ dan $c \mid d$, maka $ac \mid bd.$
4. Jika $a \mid b$ dan $b \mid c$, maka $a \mid c.$
5. $a \mid b$ dan $b \mid a$, jika dan hanya jika $a = \pm b.$
6. jika $a \mid b$ dan $b \neq 0$, maka $|a| \leq |b|$
7. jika $a \mid b$ dan $a \mid c$, maka $a \mid (bx + cy)$, untuk sembarang bilangan bulat x dan y.

(Byrne, 1967).

2.2 Persekutuan Pembagi Terbesar (*Greatest Common Divisor*)

Kita mengetahui bahwa faktor-faktor 30 adalah 1, 2, 3,5, 6, 10, 15 dan 30. Faktor-faktor 105 adalah 1, 3, 5, 7,15, 21, 35, dan 105. Maka 1, 3, 5, dan 15 disebut faktor-faktor persekutuan (pembagi-pembagi bersama/ *common divisor*) dari 30 dan 105

Definisi 2.2.1

Suatu bilangan bulat d adalah faktor persekutuan dari a dan b jika dan hanya jika $d \mid a$ dan $d \mid b$ (Burton, 1998).

perlu diperhatikan bahwa jika a dan b kedua-duanya bilangan bulat yang tak nol, maka a dan b hanya memiliki sejumlah faktor terbatas saja. Dengan kata lain himpunan faktor persekutuan dari a dan b terbatas. Hal itu disebabkan faktor-faktor persekutuan dari a dan b tidak akan lebih besar dari bilangan yang terbesar diantar a dan b. tetapi jika a atau b sama dengan 0, himpunan semua faktor persekutuannya tak terbatas. Karena 1 membagi semua bilangan, maka 1 merupakan faktor persekutuan dua bilangan bulat sembarang a dan b. oleh karena itu setiap pasangan bulat sembarang selalu memiliki faktor persekutuan. Karena elemen-elemen himpunan faktor pembagi persekutuan dari a dan b adalah bilangan-bilangan bulat maka himpunan ini mempunyai elemen terbesar yang biasa disebut faktor persekutuan terbesar (Burton, 1998).

Definisi 2.2.2

Jika a dan b bilangan-bilangan bulat yang tak nol, d adalah membagi persekutuan terbesar dari a dan b (ditulis "(a, b)") jika dan hanya jika d faktor persekutuan dari a dan b, jika c merupakan faktor persekutuan dari a dan b, maka $c \leq d$ (Baum, 1990).

Teorema 2.2.3

Jika $(a, b) = d$ maka $(a : d, b : d) = 1$

Perlu diketahui bahwa $(a: d)$ dan $(b : d)$ adalah bilangan-bilangan bulat yang diperoleh dari $(a, b) = d$, yang berarti $d \mid a$ dan $d \mid b$ yang berturut-turut menghasilkan $a = dm$ dan $b = dn$ untuk semua m dan n. selanjutnya apabila $(a, b) = 1$ maka dinyatakan bahwa a dan b saling prima.

Teorema 2.2.4

1. jika $b = q\ a + r$ dimana $(b, a) = (a, r)$
2. jika gcd $(a, b) = d$ maka bilangan x dan y sehingga $ax + by = d$
3. misalkan $a \mid c$ dan $b \mid c$ dengan gcd$(a, b) = 1$, maka $ab \mid c$.

Definisi 2.2.5

dua bilangan bulat a dan b, dimana keduanya tidak nol, maka disebut relatif prima jika setiap gcd$(a, b) = 1$ (Burton, 1998).

Teorema 2.2.6

Diketahui a dan b adalah bilangan bulat, keduanya tidak nol. Maka a dan b relatif prima jika dan hanya jika terdapat bilangan bulat x dan y yang memenuhi persamaan $1 = ax + by$.

Akibat 2.2.7

Jika gcd $(a, b) = d$, maka gcd $(a/d,\ b/d) = 1$ (Burton, 1998).

2. 3 Bilangan Prima

Definisi 2.3.1

Bilangan bulat $p > 1$ disebut bilangan prima jika hanya terdapat faktor pembaginya 1 dan p sendiri. Bilangan bulat yang lebih besar dari 1 dan bukan bilangan prima disebut bilangan komposit (Burton, 1998).

$2,\ 3, 5, 7, 11, 13, 17$ adalah bilangan prima pertama. Sedangkan $4, 6, 8, 9, 10, 12,$ adalah contoh bilangan komposit. Perlu diketahui juga, bahwa 1 bukan merupakan bilangan prima maupun bilangan komposit.

Teorema 2.3.2

1. Suatu bilangan bulat n, dimana $n > 1$ dapat dibagi oleh bilangan prima.
2. Jika p adalah bilangan prima dan $p \mid ab$, maka $p \mid a$ dan $p \mid b$.

Teorema 2.3.3

1. Jika p adalah bilangan prima dan $p \mid a_1, a_1, \ldots, a_n$, maka $p \mid a_k$ untuk beberapa nilai k dimana $1 \leq k \leq n$
2. Jika $p,\ q_1, q_2, \ldots, q_n$ semua adalah bilangan prima dan $p \mid q_1, q_2, \ldots, q_n$, diman $p = q_k$ untuk setiap k dimana $1 \leq k \leq n$.

Teorema 2.3.4 Teorema Dasar Aritmatika

Untuk sembarang bilangan bulat $n > 1$ dapat dinyatakan sebagai hasil kali dari bilangan prima serta dinyatakan dalam bentuk kanonik

$$n = p_1^{a_1}\, p_2^{a_2} \ldots p_k^{a_k}$$

Dimana $a_1, a_2, \ldots, a_k$ bilangan bulat positif dan $p_1, p_2, \ldots, p_k$ merupakan bilangan prima, dan $p_1 < p_2 < \ldots < p_k$.

Teorema 2.3.5

1. Jika n bilangan komposit, maka n memiliki faktor k sedemikian sehingga $1 < k \leq \sqrt{n}$.

2. Untuk setiap bilangan komposit n, terdapat bilangan prima p sedemikian sehingga $\leq \sqrt{n}$.

Teorema 2.3.6

Jika p_n merupakan bilangan prima ke-n, maka $p_n \leq 2^{2^{n-1}}$

Akibat 2.3.7

Untuk $n \geq 1$, setidaknya ada $n + 1$ bilangan prima kurang dari 2^{2^n}.

Lemma 2.3.8

Hasil kali dari dua bilangan bulat atau lebih yang merunut pada persamaan $4n + 1$ adalah sebuah bilangan prima

Teorema 2.3.9

Terdapat bilangan prima tak hingga yang sesuai mengikuti persamaan $4n + 3$

3.4 Kekongruensian Modulo m

Definisi 2.4.1

misalkan m bilangan bulat positif, jika a dan b bilangan bulat, maka a kongruen dengan b modulo m (ditulis $a \equiv b \pmod{m}$) jika dan hanya jika m membagi $(a - b)$ atau ditulis $m \mid (a - b)$. hal ini berarti $a - b = km$, untuk suatu bilangan bulat k. jika m tidak membagi $a - b$ maka dikatakan a tidak kongruen dengan b modulo m.

Teorema 2.4.2

1. $a \equiv b \pmod{m}$ jika dan hanya jika terdapat bilangan k sehingga $a = mk + b$.
2. setiap bilangan bulat modulo dengan tepat satu diantara $0, 1, 2, 3, \ldots,$ $(m - 1)$

(Burton, 1998).

Definisi 2.4.3

Pada $a \equiv r \pmod{m}$ dengan $0 \leq r < m$, maka r disebut residu terkecil dari $a \pmod{m}$. Untuk kongruen ini, $\{0, 1, 2, 3, \ldots, (m - 1)\}$ disebut himpunan residu terkecil modulo m (Burton, 1998).

Teorema 2.4.4

$a \equiv b \pmod{m}$, maka a dan b memiliki sisa yang sama jika dibagi m.

Definisi 2.4.5

himpunan bilangan bulat $r_1, r_2, \ldots, r_m$ disebut sistem residu lengkap modulo m jika dan hanya jika setiap bilangan bulat kongruen modulo m dengan satu dan hanya satu diantara $r_1, r_2, \ldots,$ atau r_m (Burton, 1998).

Teorema 2.4.6

diketahui $m > 1$, serta a, b, c, d merupakan sembarang bilangan bulat. Maka berlaku,

1. $a \equiv b \pmod{m}$
2. jika $a \equiv b \pmod{m}$, maka $b \equiv a \pmod{m}$
3. jika $a \equiv b \pmod{m}$ dan $b \equiv c \pmod{m}$, maka $a \equiv c \pmod{m}$
4. jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka $a + c = b + d \pmod{m}$ dan $ac = bd \pmod{m}$
5. jika $a \equiv b \pmod{m}$, maka $a + c = b + c \pmod{m}$ dan $ac + bc \pmod{m}$.
6. jika $a \equiv b \pmod{m}$, maka $a^k \equiv b^k \pmod{m}$ untuk setiap bilangan bulat k

Teorema 2.4.7

1. Jika $ca \equiv cb \pmod{m}$, lalu $a \equiv b \pmod{m/d}$, maka $d = gcd\,(c, n)$
2. Jika $ca \equiv cb \pmod{n}$ dan gcd $(c, n) = 1$, maka $a \equiv b \pmod{n}$.
3. Jika $ca \equiv cb \pmod{p}$ dan $p \nmid c$, dimana p merupakan bilangan prima, maka $a \equiv b \pmod{p}$

(Burton, 1998).

2. 5 Teori Kongruensi Linear

Definisi 2.5.1

Kongruensi linear $ax \equiv b \pmod{n}$ merupakan solusi jika dan hanya jika $d \mid b$, dimana $d = \gcd(a, n)$. jika $d \mid b$, maka d merupakan solusi yang saling tak kongruen terhadap modulo n.

Teorema 2.5.2

Jika gcd (a, n) = 1, maka kongruensi linear $ax \equiv b \pmod{n}$ merupakan solusi unik modulo n (Burton, 1998).

2.6 Teori Kuadrat Residu

Definisi 2.6.1

Diketahui p bilangan prima ganjil dan gcd(a, p) = 1. Jika kongruensi kuadrat $x^2 \equiv a \pmod{p}$ adalah solusi, maka a disebut sebagai residu kuadrat dari p. selainnya disebut tak residu kuadrat dari p (Burton, 1998).

2.7 Bilangan Kuadrat Sempurna

Definisi 2.7.1

Bilangan kuadrat sempurna adalah bilangan bulat n yang dapat dinyatakan sebagai $n = m^2$dimana m adalah bilangan bulat (Burton, 1998).

2.8 Bilangan Bulat Kuadrat Bebas (*Square-Free*)

Definisi 2.8.1

Suatu bilangan bulat dikatakan kuadrat bebas jika bilangan tersebut tidak dapat dibagi oleh kuadrat dari bilangan bulat yang lebih dari 1. Syaratnya adalah

1. bilangan bulat $n > 1$ adalah kuadrat bebas jika dan hanya jika *n* dapat difaktorkan di dalam hasil kali prima yang berbeda.

2. Setiap bilangan bulat $n > 1$ adalah hasil kali dari bilangan bulat kuadrat bebas dan berpangkat sempurna.

(Burton, 1998).

2. 9 Teori Fermat

Definisi 2.9.1

Jika p adalah bilangan prima, dan a adalah bilangan bulat positif, sehingga $p \nmid a$, dimana $a^{p-1} \equiv 1 \pmod{p}$.

Teorema 2.9.2

1. Jika p merupakan bilangan prima, dimana $a^p \equiv a \ (mod\ p)$ untuk setiap bilangan bulat a
2. Jika p dan q merupakan bilangan prima yang berbeda dengan $a^p \equiv a \ (mod\ q)$ dan $a^q \equiv a \ (mod\ p)$, maka $a^{pq} \equiv a \ (mod\ pq)$

(Baum, 1990).

2. 10 Teorema Wilson

Definisi 2.10.1

Jika p adalah bilangan prima, maka $(p - 1)! \equiv -1 \pmod{p}$ (Burton, 1998).