

Matematika Diskrit
[KOMS119602] - 2022/2023

7 - Teori Bilangan

Dewi Sintiar

Prodi D4 Teknologi Rekayasa Perangkat Lunak
Universitas Pendidikan Ganesha

Week 7 (Oktober 2022)

Bagian 1: Keterbagian

Keterbagian

Teorema

Misal $a, b, c \in \mathbb{Z}$, dimana $a \neq 0$. Maka:

1. jika $a|b$ dan $a|c$, maka $a|(b + c)$;
2. jika $a|b$ dan $a|bc$ untuk $\forall c \in \mathbb{Z}$;
3. jika $a|b$ dan $b|c$, maka $a|c$.

Corollary

Jika $a, b, c \in \mathbb{Z}$ dimana $a \neq 0$, sedemikian sehingga $a|b$ dan $a|c$.
Maka untuk $\forall m, n \in \mathbb{Z}$:

$$a|(mb + nc)$$

Algoritma pembagian

Teorema

Misalkan $a \in \mathbb{Z}$ dan $d \in \mathbb{Z}_+$. Maka terdapat tepat satu pasangan bilangan bulat q dan r dimana $0 \leq r < d$, sedemikian sehingga

$$a = dq + r$$

- ▶ d disebut **pembagi**;
- ▶ a disebut **dividen**;
- ▶ q disebut **quotient**;
- ▶ r disebut **sisanya (remainder)**.

Notasi:

$$q = a \operatorname{div} d, \quad r = a \operatorname{mod} d$$

Latihan

1. Tentukan hasil bagi dan sisa bagi dari **101 dibagi 11**.
2. Tentukan hasil bagi dan sisa bagi dari **-11 dibagi 3**.

Aritmetika modulo

Misalkan $a, b \in \mathbb{Z}$, dan $m \in \mathbb{Z}_+$. Maka dikatakan bahwa a kongruen dengan b modulo m jika m habis membagi $a - b$.

Notasi:

$a \equiv b \pmod{m}$ mengindikasikan a kongruen dengan b modulo m , dan ini disebut kekongruenan/kongruensi.

Jika a dan b tidak kongruen modulo m , dinotasikan dengan:

$$a \not\equiv b \pmod{m}$$

$a \equiv b \pmod{m}$ versus $a \bmod m$

$a \equiv b \pmod{m}$ versus $a \bmod m$

$a \equiv b \pmod{m}$ menyatakan sebuah relasi pada bilangan bulat.

$a \bmod m$ menyatakan sebuah fungsi.

Teorema

Misalkan $a, b \in \mathbb{Z}$, dan $m \in \mathbb{Z}_+$. Maka:

$a \equiv b \pmod{m}$ jika dan hanya jika $a \bmod m = b \bmod m$

$a \equiv b \pmod{m}$ versus $a \bmod m$

$a \equiv b \pmod{m}$ menyatakan sebuah relasi pada bilangan bulat.

$a \bmod m$ menyatakan sebuah fungsi.

Teorema

Misalkan $a, b \in \mathbb{Z}$, dan $m \in \mathbb{Z}_+$. Maka:

$a \equiv b \pmod{m}$ jika dan hanya jika $a \bmod m = b \bmod m$

Teorema

Misalkan $a, b \in \mathbb{Z}$, dan $m \in \mathbb{Z}_+$. Maka:

$a \equiv b \pmod{m}$ jika $\exists k \in \mathbb{Z}$ sedemikian sehingga $a = b + km$

Aritmetika modulo

Teorema

Misal $m \in \mathbb{Z}_+$. Jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka:

$$a + c \equiv b + d \pmod{m} \quad \text{dan} \quad ac \equiv bd \pmod{m}$$

Corollary

Misalkan $a, b \in \mathbb{Z}$, dan $m \in \mathbb{Z}_+$. Maka:

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

dan

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Latihan

Soal 1.

Diketahui bahwa $7 \equiv 2 \pmod{5}$ dan $11 \equiv 1 \pmod{5}$.

Tentukan kongruensi dari $77 \pmod{5}$ berdasarkan relasi tersebut.

Soal 2.

Bagian 2: Representasi integer (bilangan bulat)

Representasi integer (bilangan bulat)

Misalkan $b \in \mathbb{Z}$ dan $b > 1$. Jika $n \in \mathbb{Z}_+$, maka n dapat dituliskan sebagai:

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$$

dimana $k \in \mathbb{Z}_{\geq 0}$, $a_0, a_1, \dots, a_k \in \mathbb{Z}_{\geq 0}$ dan kurang dari b , serta $a_k \neq 0$.

Ekspansi biner

Bagaimana menyatakan $(1\ 0101\ 1111)_2$ dalam ekspansi biner?

Ekspansi biner

Bagaimana menyatakan $(1\ 0101\ 1111)_2$ dalam ekspansi biner?

Solusi:

$$\begin{aligned}(1\ 0101\ 1111)_2 &= 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 \\ &\quad + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 \\ &= 351\end{aligned}$$

Ekspansi oktal

Bagaimana menyatakan $(7016)_8$ dalam ekspansi biner?

Ekspansi oktal

Bagaimana menyatakan $(7016)_8$ dalam ekspansi biner?

Solusi:

Gunakan definisi sebelumnya dengan mengambil nilai $b = 8$.

$$(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$$

Ekspansi oktal

Bagaimana menyatakan $(7016)_8$ dalam ekspansi biner?

Solusi:

Gunakan definisi sebelumnya dengan mengambil nilai $b = 8$.

$$(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$$

Dalam ekspansi heksadesimal, digunakan 16 digit, yaitu:

0, 1, 2, 3, 4, 5, 6, 7

Ekspansi heksadesimal

Dalam ekspansi heksadesimal, digunakan 16 digit, yaitu:

$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$

dimana digit A hingga F merepresentasikan bilangan 10 hingga 15.

Ekspansi heksadesimal

Dalam ekspansi heksadesimal, digunakan 16 digit, yaitu:

$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$

dimana digit A hingga F merepresentasikan bilangan 10 hingga 15.

Bagaimana menyatakan $(2AE0B)_{16}$ dalam ekspansi biner?

Ekspansi heksadesimal

Dalam ekspansi heksadesimal, digunakan 16 digit, yaitu:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *A*, *B*, *C*, *D*, *E*, *F*

dimana digit *A* hingga *F* merepresentasikan bilangan 10 hingga 15.

Bagaimana menyatakan $(2AE0B)_{16}$ dalam ekspansi biner?

Solusi:

Gunakan definisi sebelumnya dengan mengambil nilai $b = 8$.

$$(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$$

Bagian 3: Konversi ekspansi bilangan biner, oktal, dan heksadesimal

Algoritma

Bagaimana mengkonstruksi ekspansi basis b dari suatu integer n ?

Langkah 1: Bagi n dengan b untuk mendapatkan hasil bagi dan sisa bagi, yakni:

$$n = bq_0 + a_0, \quad 0 \leq a_0 \leq b$$

Sisa a_0 adalah digit paling kanan dari ekspansi n .

Langkah 2: Bagi q_0 dengan b sehingga diperoleh:

$$q_0 = bq_1 + a_1, \quad 0 \leq a_1 < b$$

a_1 adalah digit kedua dari kanan dari ekspansi n .

Langkah berikutnya: Lanjutkan proses tersebut, dengan membagi secara berurutan hasil bagi dengan b . Proses ini dihentikan ketika hasil baginya adalah 0.

Output: Rangkaian digit yang dihasilkan merupakan representasi/ekspansi bilangan n dalam basis b (ditulis dari kanan ke kiri).

Latihan 1

Temukan ekspansi oktal dari $(12345)_{10}$.

Latihan 1

Temukan ekspansi oktal dari $(12345)_{10}$.

Solusi:

$$12345 = 8 \cdot 1543 + 1$$

$$1543 = 8 \cdot 192 + 7$$

$$192 = 8 \cdot 24 + 0$$

$$24 = 8 \cdot 3 + 0$$

$$3 = 8 \cdot 0 + 3$$

Jadi, $(12345)_{10} = (30071)_8$.

Latihan 2

Temukan ekspansi heksadesimal dari $(177130)_{10}$.

Latihan 2

Temukan ekspansi heksadesimal dari $(177130)_{10}$.

Solusi:

$$177130 = 16 \cdot 11070 + 10$$

$$11070 = 16 \cdot 691 + 14$$

$$691 = 16 \cdot 43 + 3$$

$$43 = 16 \cdot 2 + 11$$

$$2 = 16 \cdot 0 + 2$$

Sisa pembagian terurut dari operasi di atas adalah: 10, 14, 3, 11, 2 sehingga:

$$(177130)_{10} = (2B3EA)_{16}$$

Latihan 3

Temukan ekspansi biner dari $(241)_{10}$

Latihan 3

Temukan ekspansi biner dari $(241)_{10}$

Solusi:

$$241 = 2 \cdot 120 + 1$$

$$120 = 2 \cdot 60 + 0$$

$$60 = 2 \cdot 30 + 0$$

$$30 = 2 \cdot 15 + 0$$

$$15 = 2 \cdot 7 + 1$$

$$7 = 2 \cdot 3 + 1$$

$$3 = 2 \cdot 1 + 1$$

$$1 = 2 \cdot 0 + 1$$

Sisa pembagian terurut dari operasi di atas adalah: 1, 0, 0, 0, 1, 1, 1, 1, sehingga:

$$(241)_{10} = (1111\ 0001)_2$$

Tabel konversi

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Penjumlahan bilangan bulat

Contoh

Jumlahkan $a = (1110)_2$ dan $b = (1011)_2$.

Solusi:

Penjumlahan bilangan bulat

Contoh

Jumlahkan $a = (1110)_2$ dan $b = (1011)_2$.

Solusi:

$$\begin{array}{r} 1\ 1\ 1\ 0 \\ +\ 1\ 0\ 1\ 1 \\ \hline 1\ 1\ 0\ 0\ 1 \end{array}$$

Jabarkan langkah-langkah menjumlahkan bilangan dalam basis b .

Perkalian bilangan bulat

Contoh

Hitunglah $a = (110)_2$ dan $b = (101)_2$.

Perhatikan bahwa:

$$ab_0 \cdot 2^0 = (110)_2 \cdot 1 \cdot 2^0 = (110)_2$$

$$ab_1 \cdot 2^1 = (110)_2 \cdot 0 \cdot 2^1 = (0000)_2$$

$$ab_2 \cdot 2^1 = (110)_2 \cdot 0 \cdot 2^1 = (0000)_2$$

$$\begin{array}{r} \\ \\ \hline \\ \\ 1 \\ \hline 1 \end{array}$$

Jabarkan langkah-langkah mengalikan bilangan dalam basis b .

Bagian 4: Bilangan prima dan FPB

Bilangan prima

Bilangan bulat $p > 1$ disebut **bilangan prima** jika faktor dari p hanyalah 1 dan p .

Bilangan bulat yang lebih dari 1 dan *bukan prima* disebut **bilangan komposit**.

Tugas: berikan contoh bilangan prima dan bilangan komposit.

Teorema dasar aritmetika

Teorema

Setiap bilangan bulat yang lebih dari 1 dapat dinyatakan dengan **tepat satu cara** sebagai *bilangan prima* atau *perkalian dari dua atau lebih bilangan prima*, dimana faktor-faktor primanya disusun dalam urutan tak-turun (*non-decreasing*).

Contoh

Faktorisasi prima dari 100, 641, 999, dan 1024 adalah:

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$$

$$641 = 641$$

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$$

$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$$

Menyelidiki suatu bilangan prima atau bukan

Buktikan teorema berikut

Teorema

Jika n adalah bilangan komposit, maka n memiliki faktor prima yang kurang dari atau sama dengan \sqrt{n} .

Menyelidiki suatu bilangan prima atau bukan

Buktikan teorema berikut

Teorema

Jika n adalah bilangan komposit, maka n memiliki faktor prima yang kurang dari atau sama dengan \sqrt{n} .

Latihan:

1. Tunjukkan bahwa 101 adalah bilangan prima.
2. Temukan faktorisasi prima dari 7007.

Sieve Erasthones

Contoh kasus: Bagaimanakah membuat list bilangan prima yang ≤ 100 ?

- ▶ Sesuai teorema, bilangan komposit ≤ 100 pastilah memiliki faktor prima yang ≤ 10 .
- ▶ Bilangan prima yang kurang dari 10 adalah 2, 3, 5, 7.
- ▶ Maka, bilangan prima yang ≤ 100 adalah 2, 3, 5, 7, dan bilangan di antara 1 dan 100 yang tidak habis dibagi oleh 2, 3, 5, 7.

Sieve Erastothenes

TABLE 1 The Sieve of Eratosthenes.

<i>Integers divisible by 2 other than 2 receive an underline.</i>											<i>Integers divisible by 3 other than 3 receive an underline.</i>										
1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	9	10		1	2	3	4	5	<u>6</u>	7	8	9	10	
11	<u>12</u>	13	<u>14</u>	15	<u>16</u>	17	<u>18</u>	19	<u>20</u>		11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>	
21	<u>22</u>	23	<u>24</u>	25	<u>26</u>	27	<u>28</u>	29	<u>30</u>		21	<u>22</u>	23	<u>24</u>	25	<u>26</u>	27	<u>28</u>	29	<u>30</u>	
31	<u>32</u>	33	<u>34</u>	35	<u>36</u>	37	<u>38</u>	39	<u>40</u>		31	<u>32</u>	<u>33</u>	<u>34</u>	35	<u>36</u>	<u>37</u>	<u>38</u>	39	<u>40</u>	
41	<u>42</u>	43	<u>44</u>	45	<u>46</u>	47	<u>48</u>	49	<u>50</u>		41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	49	<u>50</u>	
51	<u>52</u>	53	<u>54</u>	55	<u>56</u>	57	<u>58</u>	59	<u>60</u>		51	<u>52</u>	53	<u>54</u>	55	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>	
61	<u>62</u>	63	<u>64</u>	65	<u>66</u>	67	<u>68</u>	69	<u>70</u>		61	<u>62</u>	<u>63</u>	<u>64</u>	65	<u>66</u>	67	<u>68</u>	69	<u>70</u>	
71	<u>72</u>	73	<u>74</u>	75	<u>76</u>	77	<u>78</u>	79	<u>80</u>		71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	77	<u>78</u>	79	<u>80</u>	
81	<u>82</u>	83	<u>84</u>	85	<u>86</u>	87	<u>88</u>	89	<u>90</u>		81	<u>82</u>	83	<u>84</u>	85	<u>86</u>	87	<u>88</u>	89	<u>90</u>	
91	<u>92</u>	93	<u>94</u>	95	<u>96</u>	97	<u>98</u>	99	<u>100</u>		91	<u>92</u>	<u>93</u>	<u>94</u>	95	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>	
<i>Integers divisible by 5 other than 5 receive an underline.</i>											<i>Integers divisible by 7 other than 7 receive an underline; integers in color are prime.</i>										
1	2	3	4	5	<u>6</u>	7	8	9	<u>10</u>		1	2	3	4	5	<u>6</u>	7	8	9	<u>10</u>	
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>		11	<u>12</u>	<u>13</u>	<u>14</u>	<u>15</u>	<u>16</u>	<u>17</u>	<u>18</u>	<u>19</u>	<u>20</u>	
<u>21</u>	<u>22</u>	23	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>	29	<u>30</u>		<u>21</u>	<u>22</u>	<u>23</u>	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>	<u>29</u>	<u>30</u>	
31	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>		31	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	<u>37</u>	<u>38</u>	<u>39</u>	<u>40</u>	
41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	49	<u>50</u>		41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	<u>47</u>	<u>48</u>	49	<u>50</u>	
<u>51</u>	<u>52</u>	53	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>		<u>51</u>	<u>52</u>	<u>53</u>	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	<u>59</u>	<u>60</u>	
61	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	67	<u>68</u>	69	<u>70</u>		61	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	<u>67</u>	<u>68</u>	69	<u>70</u>	
71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	77	<u>78</u>	79	<u>80</u>		71	<u>72</u>	<u>73</u>	<u>74</u>	<u>75</u>	<u>76</u>	<u>77</u>	<u>78</u>	<u>79</u>	<u>80</u>	
<u>81</u>	<u>82</u>	83	<u>84</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>		<u>81</u>	<u>82</u>	<u>83</u>	<u>84</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	<u>89</u>	<u>90</u>	
91	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>		91	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	<u>97</u>	<u>98</u>	<u>99</u>	<u>100</u>	

FPB

Misalkan $a, b \in \mathbb{Z}$ dimana a dan b tidak keduanya 0. Bilangan terbesar d sedemikian sehingga $d|a$ dan $d|b$ disebut **faktor persekutuan terbesar (FPB)** dari a dan b .

FPB dari a dan b dinotasikan dengan $\text{fpb}(a, b)$.

Latihan

1. Tentukan fpb dari 24 dan 36
2. Tentukan fpb dari 17 dan 22

Definisi

Dua bilangan a dan b dimana $\text{fpb}(a, b) = 1$ disebut **relatif prima**.

Kelipatan persekutuan terkecil (KPK)

KPK dari dua bilangan bulat positif a dan b adalah bilangan bulat positif **terkecil** yang habis dibagi a dan b .

KPK dari a dan b dinotasikan dengan $kpk(a, b)$.

Latihan

1. Tentukan kpk dari 24 dan 36
2. Tentukan kpk dari 17 dan 22

Menghitung fpb dan kpk dengan faktorisasi prima

Misalkan faktorisasi prima dari a dan b adalah:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$
$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

Maka:

$$\text{fpb}(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

dan

$$\text{kpk}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

Latihan: Hitunglah fpb dan kpk dari 120 dan 500.

Algoritma Euclid

Lemma

Misalkan $a = bq + r$ dimana a, b, q, r adalah integer. Maka:

$$\gcd(a, b) = \gcd(b, r)$$

Bagaimana menentukan fpb(a, b) untuk suatu bilangan $a, b \in \mathbb{Z}$?

Misalkan $a, b \in \mathbb{Z}$ dengan $a \geq b$. Misalkan $r_0 = a$ dan $r_1 = b$. Maka:

$$r_0 = r_1q_1 + r_2 \quad 0 < r_2 < r_1$$

$$r_1 = r_2q_2 + r_3 \quad 0 < r_3 < r_2$$

\vdots

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_nq_n$$

Algoritma Euclid

Lemma

Misalkan $a = bq + r$ dimana a, b, q, r adalah integer. Maka:

$$\gcd(a, b) = \gcd(b, r)$$

Bagaimana menentukan $\text{fpb}(a, b)$ untuk suatu bilangan $a, b \in \mathbb{Z}$?

Misalkan $a, b \in \mathbb{Z}$ dengan $a \geq b$. Misalkan $r_0 = a$ dan $r_1 = b$. Maka:

$$r_0 = r_1q_1 + r_2 \quad 0 < r_2 < r_1$$

$$r_1 = r_2q_2 + r_3 \quad 0 < r_3 < r_2$$

\vdots

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_nq_n$$

- ▶ Apa yang menjamin bahwa sisa bagi yang terakhir adalah 0?
- ▶ Dari algoritma tersebut, berapakah nilai dari $\text{fpb}(a, b)$?

Analisis algoritma Euclid

Apa yang menjamin bahwa sisa bagi yang terakhir adalah 0?

Dari algoritma tersebut, berapakah nilai dari $\text{fpb}(a, b)$?

Analisis algoritma Euclid

Apa yang menjamin bahwa sisa bagi yang terakhir adalah 0?

Barisan sisa $a = r_0 > r_1 > r_2 > \dots \geq 0$ tidak memuat lebih dari a suku.

Dari algoritma tersebut, berapakah nilai dari $\text{fpb}(a, b)$?

Analisis algoritma Euclid

Apa yang menjamin bahwa sisa bagi yang terakhir adalah 0?

Barisan sisa $a = r_0 > r_1 > r_2 > \dots \geq 0$ tidak memuat lebih dari a suku.

Dari algoritma tersebut, berapakah nilai dari $\text{fpb}(a, b)$?

$$\begin{aligned}\text{fpb}(a, b) &= \text{fpb}(r_0, r_1) = \text{fpb}(r_1, r_2) = \dots = \text{fpb}(r_{n-2}, r_{n-1}) \\ &= \text{fpb}(r_{n-1}, r_n) = \text{fpb}(r_n, 0) = r_n\end{aligned}$$

Latihan

Tentukan fpb dari 414 dan 662 dengan menggunakan algoritma Euclid.

Latihan

Tentukan fpb dari 414 dan 662 dengan menggunakan algoritma Euclid.

Solusi:

$$662 = 414 \cdot 1 + 248$$

$$414 = 248 \cdot 1 + 166$$

$$248 = 166 \cdot 1 + 82$$

$$166 = 82 \cdot 2 + 2$$

$$82 = 2 \cdot 41 + 0$$

Jadi, $\text{fpb}(414, 662) = 2$, karena **2 adalah sisa bagi tak-nol yang terakhir.**

Teorema Bezout

Teorema

Jika a dan b adalah bilangan bulat positif, maka terdapat bilangan bulat s dan t sedemikian sehingga:

$$\text{fpb}(a, b) = sa + tb$$

Contoh

1. Nyatakan $\text{fpb}(48, 96) = 12$ sebagai kombinasi linier dari 48 dan 96.
2. Nyatakan $\text{fpb}(252, 198) = 18$ sebagai kombinasi linier dari 252 dan 198.
3. Nyatakan $\text{fpb}(75, 40) = 5$ sebagai kombinasi linier dari 75 dan 40.

Pembuktian Teorema Bezout

Ingatlah bahwa Teorema Bezout menyatakan:

Jika a dan b adalah bilangan bulat positif, maka terdapat bilangan bulat s dan t sedemikian sehingga:

$$\text{fpb}(a, b) = sa + tb$$

Coba Anda buktikan teorema tersebut secara formal. (*Hint:* gunakan algoritma Euclid.)

Bagian 5: Kongruensi

Kongruensi linier

Kongruensi linier adalah bentuk:

$$ax \equiv b \pmod{m}$$

dimana $m \in \mathbb{Z}_+$, $a, b \in \mathbb{Z}$, dan x adalah variabel.

Solusi dari kongruensi linier tersebut adalah semua bilangan bulat x yang memenuhi kongruensi tersebut.

Bagaimana menentukan solusi dari $ax \equiv b \pmod{m}$?

Kita akan cari nilai $\bar{a} \in \mathbb{Z}$ (jika ada) sedemikian sehingga $\bar{a}a \equiv 1 \pmod{m}$.

Invers modulo

Misalkan $m \in \mathbb{Z}_+$, $a, b \in \mathbb{Z}$. Suatu bilangan bulat $\bar{a} \in \mathbb{Z}$ yang memenuhi $\bar{a}a \equiv 1 \pmod{m}$ dinamakan **invers dari a modulo m** .

Teorema

Jika a dan m adalah bilangan bulat relatif prima (memiliki $\text{fpb} = 1$) dan $m > 1$, maka a memiliki invers.

Lebih lanjut, terdapat tepat satu bilangan bulat \bar{a} yang $< m$ yang merupakan invers dari a modulo m . Invers lain dari a modulo m kongruen dengan \bar{a} modulo m .

Invers modulo

Misalkan $m \in \mathbb{Z}_+$, $a, b \in \mathbb{Z}$. Suatu bilangan bulat $\bar{a} \in \mathbb{Z}$ yang memenuhi $\bar{a}a \equiv 1 \pmod{m}$ dinamakan **invers dari a modulo m** .

Teorema

Jika a dan m adalah bilangan bulat relatif prima (memiliki $\text{fpb} = 1$) dan $m > 1$, maka a memiliki invers.

Lebih lanjut, terdapat tepat satu bilangan bulat \bar{a} yang $< m$ yang merupakan invers dari a modulo m . Invers lain dari a modulo m kongruen dengan \bar{a} modulo m .

Bagaimana menentukan invers dari a modulo m untuk nilai m yang kecil?

Tugas: Buatlah beberapa (minimal 3) kongruensi linier, dan tunjukkan kebenaran teorema tersebut.

Latihan 1

Temukan invers dari 3 modulo 7 dengan cara menentukan koefisien Bézout dari 3 dan 7.

Solusi:

Karena $\text{fpb}(3, 7) = 1$, maka berdasarkan Teorema sebelumnya, 3 memiliki invers modulo 7.

Aplikasikan algoritma Euclid, sehingga pada barik akhir ditemukan:

$$7 = 2 \cdot 3 + 1$$

yang ekuivalen dengan: $-2 \cdot 3 + 1 \cdot 7 = 1$.

Ini berarti -2 dan 1 adalah koefisien Bézout dari 3 dan 7

Bagian 6: Penerapan Teori Bilangan

Aktivitas eksploratif: Penerapan Teori Bilangan

Buatlah kelompok beranggotakan 2-3 orang.

Selidiki penerapan teori bilangan dalam bidang Informatika.

1. Fungsi hashing
2. Bilangan pseudorandom
3. Digit pengecekan
4. Kriptografi
5. ...
6. ...