TEORI BILANGAN

(*Slide Acknowledgment*: Gatot Wahyudi, Adila A. Krisnadhi, Kurniawati Azizah)

Matematika Diskret 2

Fakultas Ilmu Komputer Universitas Indonesia

Agenda

- Pembagian Bilangan Bulat
- Aritmetika Modular
- Representasi Bilangan Bulat
- Bilangan Prima
- *Greatest Common Divisor* (GCD)
- Kongruensi Linear

Pengantar

- Aritmetika (ilmu hitung): cabang matematika yang mempelajari operasi dasar pada bilangan: penjumlahan, pengurangan, perkalian, dan pembagian
- Istilah aritmetika biasa dipakai dalam konteks bilangan bulat
  - ... meski operasi-operasi di atas berlaku untuk bilangan rasional, riil, dan kompleks.
- Teori bilangan: cabang matematika yang mempelajari bilangan bulat beserta segala sifat, operasi dan generalisasi yang dapat diturunkan darinya.
  - Aritmetika merupakan bagian dari teori bilangan.
- Aplikasi teori bilangan: kriptografi (penyamaran informasi), *hashing* (untuk akses informasi secara cepat), *digit error checking*

Notasi

- Himpunan seluruh bilangan **bulat**: $Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- Himpunan seluruh bilangan **bulat positif**: $Z^+ = \{1, 2, 3, \ldots\}$
- Himpunan seluruh bilangan **bulat negatif**: $Z^- = \{\ldots, -3, -2, -1\}$
- Himpunan bilangan **natural** atau bilangan **bulat nonnegatif**:
  $N = \{0, 1, 2, 3, \ldots\}$

Pembagian Bilangan Bulat

Pembagian Bilangan Bulat

- Mengapa membahas pembagian?
  - Pembagian bilangan bulat mempunyai sifat yang berbeda daripada operasi dasar lainnya
  - Jika sebuah bilangan bulat dibagi dengan bilangan bulat yang tidak nol maka hasilnya belum tentu bilangan bulat
    - 27/3 = 9 → hasil pembagian adalah bil. bulat
    - 3/2 = 1.5 → hasil pembagian bukan bil. bulat
  - Bagaimana jika kita ingin melakukan operasi pembagian agar hasilnya juga bilangan bulat?

Keterbagian

- Definisi

Misalkan ***a*** dan ***b*** adalah bilangan bulat dengan ***a* ≠ 0**
Maka ***a*** dikatakan membagi ***b*** (ditulis ***a* | *b***) jika ada sebuah bilangan bulat ***c*** sehingga ***b* = *ac***
Jika ***a* | *b*** maka ***a*** adalah sebuah **faktor** dari ***b*** sedangkan ***b*** adalah sebuah **kelipatan** dari ***a***
Jika ***a*** tidak membagi ***b*** maka dinotasikan $\boldsymbol{a \nmid b}$

Pembagian Bilangan Bulat

- Contoh
  - Apakah 5 | 100?
    - Ya, karena ada bilangan bulat 20 sehingga diperoleh 100 = 20 . 5
  - Apakah 33 | 166?
    - Tidak, karena bilangan bulat yang hasil perkaliannya paling mendekati 166 adalah 5 tetapi 166 ≠ 33 . 5

Pembagian Bilangan Bulat

- Teorema

Misalkan ***a***, ***b***, dan ***c*** adalah bilangan bulat:

1. Jika $a \mid b$ dan $a \mid c$ maka $a \mid (b + c)$
2. Jika $a \mid b$ maka $a \mid bc$ untuk semua bilangan bulat c
3. Jika $a \mid b$ dan $b \mid c$ maka $a \mid c$

Pembagian Bilangan Bulat

- Pembuktian
  - Teorema bagian kedua
    - Jika $a \mid b$ maka sesuai definisi ada sebuah bilangan bulat s sehingga $b = as$
    - Kalikan kedua ruas persamaan tersebut dengan sembarang bilangan bulat c, diperoleh $bc = asc$
    - Perhatikan bahwa $bc = a(sc)$ dimana sc adalah juga merupakan bilangan bulat
    - Karena ada bilangan bulat sc sehingga bc habis dibagi dengan a maka $a \mid bc$

Pembagian Bilangan Bulat

- Teorema

> Misalkan a, b, dan c bilangan bulat sehingga $a \mid b$ dan $a \mid c$, maka $a \mid mb + nc$ untuk setiap bilangan bulat m dan n

Pembagian Bilangan Bulat

- Pembuktian (lanjutan)
  - Dengan menggunakan teorema-teorema sebelumnya
    - Diketahui $a \mid b$ maka berlaku $a \mid mb$ untuk setiap bulangan bulat m
    - Diketahui $a \mid c$ maka berlaku $a \mid nc$ untuk setiap bilangan bulat n
    - Karena kita mendapati $a \mid mb$ dan $a \mid nc$ maka dapat diperoleh $a \mid mb + nc$

Teorema Pembagian

- Teorema

> Misalkan ***a*** adalah bilangan bulat dan ***d*** adalah bilangan bulat positif, maka terdapat bilangan-bilangan bulat yang unik ***q*** dan ***r*** dengan $0 \leq r < d$ sedemikian hingga $a = dq + r$

- Bilangan ***q*** disebut *quotient* (hasil bagi) dan ditulis ***q*** = ***a*** div ***d***
- Bilangan ***r*** disebut *remainder* (sisa hasil bagi) dan ditulis ***r*** = ***a*** mod ***d***
- Catatan
  - Teorema di atas seringkali disebut algoritma pembagian meskipun sebenarnya bukan sebuah algoritma

Teorema Pembagian

- Contoh
  - Berapakah hasil bagi dan sisa hasil bagi bilangan bulat 212 dibagi 20?
    - Karena 212 = 20.10 + 12, maka
      - Hasil bagi 212 dibagi 20 adalah 212 **div** 20 = 10
      - Sisa hasil bagi 212 dibagi 20 adalah 212 **mod** 20 = 12
  - Berapakah hasil bagi dan sisanya: -21 dibagi 4?
    - Ingat bahwa *r* tidak boleh negatif!
    - Karena -21 = 4.(-6) + 3 maka
      - Hasil bagi -21 dibagi 4 adalah -21 div 4 = -6
      - Sisa hasil bagi -21 dibagi 4 adalah -21 mod 4 = 3

Pembagian Bilangan Bulat

- Contoh
  - Jika ***n*** dan ***d*** adalah bilangan bulat positif, maka berapa banyaknya bilangan bulat positif yang habis dibagi oleh ***d*** yang tidak boleh melebihi ***n***?
    - Bilangan bulat positif yang habis dibagi ***d*** adalah semua bilangan dalam bentuk ***d.k*** di mana ***k*** adalah bilangan bulat positif juga
    - Selanjutnya bilangan bulat yang diminta tidak melebihi ***n*** maka harus memenuhi $0 < d.k \leq n$ atau $0 < k \leq n/d$
    - Dengan demikian terdapat $\lfloor n/d \rfloor$ bilangan bulat yang habis dibagi ***d*** dan nilainya tidak melebihi ***n***
    - Atau dapat juga dikatakan jawabannya adalah ***n* div *d***

Aritmetika Modular

Teorema Pembagian

- Teorema

> Sebuah bilangan bulat ***a*** dikatakan habis dibagi bilangan bulat ***d*** jika dan hanya jika ***a* mod *d* = 0**

Aritmetika Modular

- Dalam kehidupan nyata, banyak ditemukan bahwa kita seringkali hanya peduli pada sisa hasil bagi saja:
  - Ujian Tengah Semester (UTS) akan tiba pada hari ke-60 perkuliahan. Jika hari pertama perkuliahan jatuh pada hari Senin, maka UTS akan jatuh pada hari?
    - 60 adalah hari ke-60
    - 7 adalah banyaknya jenis hari yang ada
    - Jawabannya: Kamis
  - Bagaimana jika hari pertama perkuliahan jatuh pada hari Kamis? Hari apa UTS akan dimulai?
  - Bagaimana jika hari ke-60 perkuliahan hanya dengan memperhitungkan hari kerja saja? Hari apa UTS akan dimulai?

Aritmetika Modular

- Dalam kehidupan nyata, banyak ditemukan bahwa kita seringkali hanya peduli pada sisa hasil bagi saja:
  - Seorang bayi perlu diimunisasi X pada hari ke-30 kehidupannya. Jika ia lahir pada tanggal 2 Februari 2016, maka ia perlu diimunisasi pada tanggal?
    - Cara 1: (30 + 1 dibagi 29 sisanya 2)
      - 30 adalah hari ke-30
      - 1 adalah banyaknya hari di bulan Februari sebelum hari kelahirannya
      - 29 adalah banyaknya hari di bulan Februari (tahun kabisat)
    - Cara 2: (30 dibagi 28 sisanya 2)
      - 30 adalah hari ke-30
      - 28 adalah banyaknya hari di bulan Februari terhitung sejak hari kelahirannya
    - Jawaban: 2 Maret 2016

Aritmetika Modular

- Perhatikan!
  - Sisa hasil bagi bilangan 10 dibagi 3 adalah 1
  - Sisa hasil bagi bilangan 19 dibagi 3 adalah 1
  - Meskipun dua bilangan tersebut berbeda:
    - Dalam penerapan operasi modulo 3 terhadap kedua bilangan tersebut hasilnya adalah sama yaitu 1
    - Dapat dikatakan bahwa 19 kongruen dengan 10 dalam modulo 3 atau bisa ditulis:

      $19 \equiv 10 \pmod{3}$ atau $10 \equiv 19 \pmod{3}$
    - Dua bangun dalam geometri disebut kongruen bila dua bangun memiliki bentuk dan ukuran yang sama
    - Dua bilangan dalam aritmetika disebut kongruen bila dua bilangan mempunyai sisa hasil bagi yang sama

Aritmetika Modular

- Definisi

> Misalkan a dan b adalah bilangan bulat dan m adalah bilangan bulat positif, maka $a \equiv b \pmod{m}$, jika dan hanya jika $m \mid a - b$.
> Notasi $a \equiv b \pmod{m}$ dibaca "a kongruen b modulo m"

- Notasi di atas disebut kongruensi dan m disebut sebagai modulus
- Jika a tidak kongruen b modulo m maka ditulis $a \not\equiv b \pmod{m}$
- Perhatikan bahwa notasi "mod" pada $a \equiv b \pmod{m}$ dan $a \bmod m \equiv b$ mewakili dua hal yang berbeda, walaupun erat hubungannya.

Aritmetika Modular

- Teorema

Misalkan a, b bilangan bulat dan m bilangan bulat positif, maka $a \equiv b \pmod{m}$ jika dan hanya jika $a \bmod m = b \bmod m$

D.k.l., $a \equiv b \pmod{m}$ jika dan hanya jika a dan b memiliki sisa bagi yang sama ketika dibagi m.

Aritmetika Modular

- Contoh
  - Apakah $27 \equiv 3 \pmod{8}$?
    - Ya, karena $8 \mid 27 - 3$
  - Apakah $15 \equiv 33 \pmod{3}$?
    - Ya, karena $15 - 33 = -18$ dan $3 \mid -18$
  - Apakah $24 \equiv 14 \pmod{6}$?
    - Tidak, karena $24 - 14 = 10$ dan 10 tidak habis dibagi 6 ($6 \nmid 10$)

Aritmetika Modular

- Sifat-sifat kongruensi
  - Jika a, b, dan c bilangan bulat dan m bilangan bulat positif maka berlaku sifat-sifat berikut:
    - Refleksif
      - Berlaku $a \equiv a \ (mod\ m)$ dan $b \equiv b \ (mod\ m)$
    - Simetris
      - Jika $a \equiv b \ (mod\ m)$ maka $b \equiv a \ (mod\ m)$
    - Transitif
      - Jika $a \equiv b \ (mod\ m)$ & $b \equiv c \ (mod\ m)$ maka $a \equiv c \ (mod\ m)$

Aritmetika Modular

- Teorema

Misalkan ***m*** bilangan bulat positif, maka dapat dikatakan $\boldsymbol{a \equiv b \pmod{m}}$ jika dan hanya jika terdapat sebuah bilangan bulat ***k*** sedemikian hingga
$\boldsymbol{a = b + km}$

Aritmetika Modular

- Bukti
  - Jika $a \equiv b \pmod{m}$ maka m | a – b sehingga terdapat bilangan bulat k sehingga $a - b = km$. Persamaan ini dapat ditulis juga $a = b + km$
  - Sebaliknya jika terdapat bilangan bulat k sehingga $a = b + km$, maka $a - b = km$ dengan kata lain $a \equiv b \pmod{m}$
- Catatan
  - Himpunan semua bilangan bulat yang kongruen dengan bilangan bulat a modulo m disebut kelas kongruensi (*congruence class*) a modulo m

Aritmetika Modular

Definisi Congruence Class

Diberikan bilangan bulat a dan bilangan bulat positif m. **Kelas kongruensi** a **modulo** m, ditulis $[a]_m$, adalah himpunan semua bilangan bulat yang kongruen dengan a modulo m.

Contoh:

- $[0]_3 = [3]_3 = [-3]_3 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$
- $[1]_3 = [4]_3 = [-2]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$
- $[2]_3 = [5]_3 = [-1]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$

Aritmetika Modular

- Teorema

Untuk m anggota bilangan bulat positif, jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$ maka

$$a + c \equiv b + d \pmod{m}$$

dan

$$ac \equiv bd \pmod{m}$$

Aritmetika Modular

- Pembuktian
  - Karena $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$ maka terdapat bilangan bulat s dan t sehingga $a = b+sm$ dan $c = d + tm$

    $a + c \quad = (b + sm) + (d + tm)$

    $\qquad\quad = (b + d) + (s + t)\text{ m} \rightarrow$ berbentuk $x = y + km$

    $ac \quad = (b + sm)(d + tm)$

    $\qquad\quad = bd + \text{b}tm + \text{d}sm + stm^2$

    $\qquad\quad = bd + (bt + \text{ds} + stm)m \rightarrow$ berbentuk $x = y + km$

  - Dengan demikian terbukti bahwa

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

Aritmetika Modular

- Contoh

  Karena $7 \equiv 2 \pmod 5$ dan $11 \equiv 1 \pmod 5$, maka:

$$7 + 11 \equiv 2 + 1 \pmod 5$$
$$18 \equiv 3 \pmod 5$$

dan

$$7 \cdot 11 \equiv 2 \cdot 1 \pmod 5$$
$$77 \equiv 2 \pmod 5$$

Aritmetika Modular

Mencari modulo dari penjumlahan dan perkalian

- Corollary

Misalkan a dan b bilangan bulat dan m bilangan bulat positif maka:

$$(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

dan

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)\ (b \textbf{ mod } m)) \textbf{ mod } m$$

Aritmetika Modular
Hati-hati!

- Meskipun terdapat operasi penjumlahan dan perkalian yang berlaku dalam kongruensi modulo namun terdapat beberapa sifat lain yang tidak berlaku

  Ketika $ac \equiv bc \pmod{m}$ maka belum tentu berlaku $a \equiv b \pmod{m}$.

  - Contoh 1:

    $0 \,.\, 2 \equiv 1 \,.\, 2 \pmod{2}$, *namun*

    $0 \not\equiv 1 \pmod{2}$

  - Contoh 2:

    $80 \equiv 14 \pmod{6}$

    $40 \,.\, 2 \equiv 7 \,.\, 2 \pmod{6}$, *namun*

    $40 \not\equiv 7 \pmod{6}$

  Jadi, **tidak boleh** mencoret pengali di kedua sisi kongruensi.

Aritmetika Modular

Hati-hati!

Jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka apakah $a^c \equiv b^d \pmod{m}$ selalu berlaku?

- Belum tentu. Contohnya, $3 \equiv 8 \pmod{5}$ dan $6 \equiv 1 \pmod{5}$, tetapi $729 = 3^6 \not\equiv 8^1 = 8 \pmod{5}$.

Jadi, pasangan basis yang kongruen serta pasangan pangkat yang kongruen tidak menjadikan hasil pemangkatannya menjadi kongruen.

Aritmetika Modular

Aritmetika modulo *m*

- Untuk setiap bilangan bulat positif m, kita dapat definisikan himpunan Z_m yang merupakan subset Z berisi semua bilangan bulat nonnegatif yang nilainya kurang dari m.
  - $Z_m = \{0, 1, . . . , m - 1\}$.
- Mirip dengan himpunan bilangan bulat, kita dapat definisikan operasi penjumlahan dan perkalian pada Z_m.
- Di SD/SMP/SMA, aritmetika ini sering disebut aritmetika jam khususnya jika $m = 12$ atau $m = 24$.
- Bagaimana jika $m = 2$?

Aritmetika Modular

Aritmetika modulo *m*

Definisi

Diberikan suatu bilangan bulat positif m. Maka, pada himpunan Z_m dapat didefinisikan:

- Penjumlahan $+_m$, yakni $a +_m b = (a + b)$ **mod** m
- Perkalian $\cdot_m$, yakni $a \cdot_m = (a \cdot b)$ **mod** m.

Contoh: Pada himpunan Z_{11} dapat dihitung bahwa:

- $7 +_{11} 9 = (7 + 9)$ **mod** $11 = 16$ **mod** $11 = 5$.
- $7 \cdot_{11} 9 = (7 \cdot 9)$ **mod** $11 = 63$ **mod** $11 = 8$.

Aritmetika Modular

Sifat-sifat operasi $+_m$ dan $\cdot_m$ I

- **Tertutup (Closure)**. Jika $a, b \in Z_m$, maka $(a +_m b) \in Z_m$ dan $(a \cdot_m b) \in Z_m$.
- **Asosiatif**. Jika $a, b, c \in Z_m$, maka $(a +_m b) +_m c = a +_m (b +_m c)$ dan $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
- **Komutatif**. Jika $a, b \in Z_m$, maka $a +_m b = b +_m a$ dan $a \cdot_m b = b \cdot_m a$.
- Memiliki **elemen identitas**.
  - Terdapat suatu $c \in Z_m$ sehingga $a +_m c = c +_m a = a$ untuk setiap $a \in Z_m$. Biasanya bilangan c di sini dinamakan nol (zero) dengan simbol 0.
  - Terdapat suatu $c \in Z_m$ sehingga $a \cdot_m c = c \cdot_m a = a$ untuk setiap $a \in Z_m$. Biasanya bilangan c di sini dinamai dengan simbol 1.

Aritmetika Modular

Sifat-sifat operasi $+_m$ dan $\cdot_m$ I

- **Invers penjumlahan**. Jika $a \neq 0$ elemen dari Z_m, maka $m-a$ adalah invers penjumlahan dari a modulo m, yakni $a +_m (m-a) = 0$. Lalu berlaku bahwa 0 adalah invers penjumlahan dari dirinya sendiri, yakni $0 +_m 0 = 0$.
- **Distributif**. Jika $a, b, c \in Z_m$, maka $a \cdot_m (b +_m c) = (a \cdot_m b) + (a \cdot_m c)$ dan $(a +_m b) \cdot_m c = (a \cdot_m c) + (b \cdot_m c)$.

Aritmetika Modular

- Aplikasi kongruensi
  - Fungsi hashing
    - Untuk *load balancing* penyimpanan data, *load balancing* beban *request* ke beberapa server, dll.
  - Pembangkitan bilangan *pseudorandom*
    - Untuk membangkitkan bilangan random oleh komputer
  - Kriptologi
    - Sandi Caesar yang legendaris menggunakan kongruensi modulo misalnya $f(p) = (p + 1) \bmod 26$
      - J MPWF ZPT
    - Bagaimana mengetahui pesan aslinya?
      - Gunakan fungsi $f(p) = (p - 1) \bmod 26$

Representasi Bilangan Bulat

Representasi Bilangan Bulat

- Representasi bilangan bulat tergantung basis yang dipilih.
- Setiap bilangan bulat positif $b > 1$ dapat digunakan sebagai basis.
- Representasi dalam basis b ditulis dengan menggunakan b buah simbol yang berbeda.
- Basis yang banyak dipakai/dikenal:
    - basis 10 (desimal) ~ 10 simbol: 0-9
    - basis 2 (biner) ~ 2 simbol: 0-1
    - basis 8 (oktal) ~ 8 simbol: 0-7
    - basis 16 (heksadesimal) ~ 16 simbol: 0-9, A-F .

Representasi Bilangan Bulat

- Teorema

Diberikan bilangan bulat positif ***b* > *1*** sebagai basis, maka setiap bilangan positif ***n*** dapat dinyatakan secara unik dalam bentuk

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

yang mana ***k*** bilangan bulat nonnegatif, a_0, a_1, . . . , a_k bilangan bulat nonnegatif yang lebih kecil dari ***b***, serta $a_k \neq 0$

- Bilangan bulat positif ***b*** menjadi basis bilangan
- Representasi bilangan ***n*** dalam basis ***b*** disebut ekpansi basis ***b*** dari ***n***.
- Ekspansi ***n*** dalam basis ***b*** dinotasikan dengan: $(a_k a_{k-1} \ldots a_1 a_0)_b$
  - Contoh: $(175)_8 = 1 . 8^2 + 7 . 8^1 + 5 . 8^0$

Representasi Bilangan Bulat

- Ekspansi bilangan bilangan bulat yang sering digunakan

Basis	Nama Ekspansi	Digit yang digunakan
10	DESIMAL	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
8	OKTAL	0, 1, 2, 3, 4, 5, 6, 7
2	BINER	0, 1
16	HEKSADESIMAL	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Ekspansi Basis *b* ke Ekspansi Desimal

- Carilah ekspansi desimal dari $(101101)_2$

$$
\begin{aligned}
(101101)_2 &= 1.2^5 + 0.2^4 + 1.2^3 + 1.2^2 + 0.2^1 + 1.2^0 \\
&= 32 + 0 + 8 + 4 + 1 \\
&= (45)_{10}
\end{aligned}
$$

- Carilah ekspansi desimal dari $(B15A)_{16}$

$$
\begin{aligned}
(B15A)_{16} &= 11.16^3 + 1.16^2 + 5.16^1 + 10.16^0 \\
&= (45402)_{10}
\end{aligned}
$$

- Carilah ekspansi desimal dari $(234)_8$

$$
\begin{aligned}
(234)_8 &= 2.8^2 + 3.8^1 + 4.8^0 \\
&= (156)_{10}
\end{aligned}
$$

Ekspansi Desimal ke Ekspansi Basis *b*

- Carilah ekspansi oktal dari $(1705)_{10}$!
  - Perhatikan:

$$
\begin{aligned}
1705 &= 8 \cdot 213 + 1 \\
213 &= 8 \cdot 26 + 5 \\
26 &= 8 \cdot 3 + 2 \\
3 &= 8 \cdot 0 + 3
\end{aligned}
$$

  - Jadi, $(1705)_{10} = (3251)_8$
- Carilah ekspansi biner dari $(9009)_{10}$!
- Carilah ekspansi heksadesimal dari $(331771)_{10}$!

Ekspansi Desimal ke Ekspansi Basis b

Carilah expansi heksadesimal dari $(331771)_{10}$.

$$\begin{aligned}
331771 &= 16 \cdot 20735 + 11 \\
20735 &= 16 \cdot 1295 + 15 \\
1295 &= 16 \cdot 80 + 15 \\
80 &= 16 \cdot 5 + 0 \\
5 &= 16 \cdot 0 + 5
\end{aligned}$$

Hasilnya $(50FFB)_{16}$ karena B dan F masing-masing adalah heksadesimal digit untuk 11 dan 15.

Konversi antara ekspansi biner, oktal, dan heksadesimal

- Konversi bilangan antar dua basis non-desimal b_1 dan b_2
  1. ubah ekspansi basis b_1 ke basis desimal.
  2. ubah hasilnya menjadi ekspansi basis b_2.
- Konversi antar ekspansi biner, oktal, dan heksadesimal (metode cepat):
  - 3 digit biner untuk 1 digit oktal dan 4 digit biner untuk 1 digit heksadesimal
  - diproses dari kanan.

$$(11111010111100)_2 = \underbrace{011}_{3_8}\,\underbrace{111}_{7_8}\,\underbrace{010}_{2_8}\,\underbrace{111}_{7_8}\,\underbrace{100}_{4_8} = (37274)_8$$

$$= \underbrace{0011}_{3_{16}}\,\underbrace{1110}_{E_{16}}\,\underbrace{1011}_{B_{16}}\,\underbrace{1100}_{C_{16}} = (3E\ B\ C\ )_{16}$$

$$(567)_8 = (101\ 110\ 111)_2$$

$$(D8A)_{16} = (1101\ 1000\ 1010)_2$$

Fungsi *floor* dan *ceiling*

- Fungsi *floor*:
  $\lfloor x \rfloor$ = bilangan bulat terbesar yang kurang dari atau sama dengan x.
- Fungsi *ceiling*:
  $\lceil x \rceil$= bilangan bulat terkecil yang lebih dari atau sama dengan x.

Teorema

Untuk bilangan bulat a dan bilangan bulat $d > 1$, berlaku:

- a **div** $d = \left\lfloor \frac{a}{d} \right\rfloor$
- a **mod** $d = a - d \left\lfloor \frac{a}{d} \right\rfloor$

Bukti: (latihan)

Pemangkatan Modular

- Permasalahan umum dalam *cryptography*
  - Menemukan solusi untuk b^n **mod** m sangat penting
    - Kondisinya ***b***, ***n***, dan ***m*** adalah bilangan bulat yang besar
  - Cobalah hitung:
    - 3^{644} mod 645 = ?
      - Jika kita menghitung 3^{644} terlebih dahulu tentu akan sangat tidak efisien
  - Daripada menggunakan cara dasar yang tidak efisien tersebut, kita dapat menggunakan algoritma ekspansi biner dari eksponen ***n*** yang ada dalam b^n **mod** m

Pemangkatan Modular

- Ide Dasar
  - Kita akan menggunakan ekspansi biner dari ***n*** untuk menghitung $\boldsymbol{b^n}$
  - Ingat bahwa ekspansi biner ***n*** berbentuk:

    $n = (a_{k-1} \ldots a_1 a_0)_2 = a_{k-1}2^{k-1} + \ldots + a_1 2^1 + a_0$
  - Dengan demikian bentuk $\boldsymbol{b^n}$ menjadi:

$$\boldsymbol{b^n = b^{a_{k-1}.2^{k-1} + \cdots + a_1.2^1 + a_0}}$$

$$\boldsymbol{b^n = b^{a_{k-1}.2^{k-1}} . \cdots . b^{a_1.2^1} . b^{a_0}}$$

Pemangkatan Modular

- Contoh:
  - Misalkan untuk bilangan 3^{11}
  - Perhatikan bahwa nilai ***n* = 11**, ekspansi biner dari $11 = (1011)_2$
  - Dengan demikian bentuk 3^{11} menjadi:

$$3^{11} = 3^{1.2^3+0.2^2+1.2^1+1.2^0}$$

$$3^{11} = 3^{1.2^3}.3^{0.2^2}.3^{1.2^1}.3^{1.2^0}$$

$$3^{11} = 3^8.3^0.3^2.3^1$$

Pemangkatan Modular

```
procedure : modexp(b: integer, m: positive integer, n = (a_{k-1}a_{k-2}…a_1a_0)_2)

x := 1
power := b mod m
for i := 0 to k-1
    if a_i = 1 then x := (x . power) mod m
    power := (power . power) mod m
return x{x equals b^n mod m}
```

Pemangkatan Modular

- Contoh
  - Berapakah 3^{644} mod 645?
- Solusi
  - Diketahui $b = 3$, $n = 644$, $m = 645$
  - Ekspansi biner dari n adalah sebagai berikut:
    - $644 = (1010000100)_2$
  - Selanjutnya kita gunakan algoritma *modular exponentiation* untuk mencari jawabannya

Pemangkatan Modular

i	a_i	x	*calculate power*	*power*
0	0	1	3^2 mod 645 = 9 mod 645 = 9	9
1	0	1	9^2 mod 645 = 81 mod 645 = 81	81
2	1	1 . 81 mod 645 = **81**	81^2 mod 645 = 6,561 mod 645 = 111	111
3	0	81	111^2 mod 645 = 12,321 mod 645 = 66	66
4	0	81	66^2 mod 645 = 4,356 mod 645 = 486	486
5	0	81	486^2 mod 645 = 236,196 mod 645 = 126	126
6	0	81	126^2 mod 645 = 15,876 mod 645 = 396	396
7	1	81 . 396 mod 645 = **471**	396^2 mod 645 = 156,816 mod 645 = 81	81
8	0	471	81^2 mod 645 = 6561 mod 645 = 111	111
9	1	471 . 111 mod 645 = **36**	STOP	STOP

Jadi, 3^{644} mod 645 = 36