# Teori Bilangan

**TK13029**
**COMPUTATION II**

# Tujuan Pembelajaran dan Materi

- Mempelajari himpunan bilangan bulat dan propertinya
- Materi:
  - Pembagian dan Modular Arithmetic
  - Representasi Bilangan Bulat
  - Bilangan Prima dan Greatest Common Divisor
  - Kongruensi

# Pembagian dan Modular Arithmetic

# Pembagian

- Jika $a$ dan $b$ adalah bilangan bulat dimana $a \neq 0$, dikatakan $a$ membagi habis $b$ jika ada bilangan bulat $c$ sehingga $b = ac$.
  - $a$ disebut sebagai faktor atau pembagi $b$
  - $b$ disebut kelipatan dari $a$
  - $a \mid b$ : $a$ membagi $b$
  - $a \nmid b$ : $a$ tidak membagi $b$
  - Jika $a \mid b$ dan $a \mid c$, maka $a \mid (b + c)$
  - Jika $a \mid b$, maka Jika $a \mid bc$, untuk semua bilangan bulat $c$
  - Jika $a \mid b$ dan $b \mid c$, maka $a \mid c$
- Contoh: 3 | 7 dan 3 | 12
  - $3 \nmid 7$ dan $3 \mid 12$

# Algoritma Pembagian

- Diketahui $a$ adalah bilangan bulat dan $d$ bilangan bulat positif. Terdapat bilangan bulat unik $q$ dan $r$, dengan $0 \leq r < d$, sehingga $a = dq + r$
  - $a$ adalah bilangan yang dibagi (*dividen*)
  - $d$ adalah pembagi (*divisor*)
  - $q$ adalah hasil bagi (*quotient*)
  - $r$ adalah sisa bagi (*reminder*)
  - $q = a \text{ div } d$ dan $r = a \bmod d$
- Contoh: tentukan
  - $q$ dan $r$ untuk $101$ dibagi $11$
    - $101 = 11(9) + 2$, $q = 9$ dan $r = 2$
  - $q$ dan $r$ untuk $-11$ dibagi $3$
    - $-11 = 3(-4) + 1$, $q = -4$ dan $r = 1$ ($r$ tidak boleh negatif karena $0 \leq r < 3$)

# Modular Arithmetic (1)

- Jika $a$ dan $b$ adalah bilangan bulat dan $m$ bilangan bulat positif, maka $a$ dikatakan kongruen $b$ modulo $m$ jika $m$ membagi $a - b$.
    - $a$ kongruen $b$ modulo $m$ : $a \equiv b (\mathrm{mod}\ m)$
    - $a$ tidak kongruen $b$ modulo $m$ : $a \not\equiv b (\mathrm{mod}\ m)$
    - $a \equiv b (\mathrm{mod}\ m)$ jika dan hanya jika $a \bmod m = b \bmod m$
    - $a \equiv b (\mathrm{mod}\ m)$ jika dan hanya jika terdapat bilangan bulat $k$ sehingga $a = b + km$
- Contoh:
    - apakah 17 kongruen 5 modulo 6?
        - 6 membagi habis (17 - 5) = 12
    - apakah 24 kongruen 14 modulo 6?
        - 6 tidak membagi habis (24 - 14) = 10

# Modular Arithmetic (2)

- Diketahui $m$ bilangan bulat positif. Jika $a \equiv b (\mathrm{mod}\ m)$ dan $c \equiv d (\mathrm{mod}\ m)$, maka
  - $a + c \equiv b + d (\mathrm{mod}\ m)$
  - $ac \equiv bd (\mathrm{mod}\ m)$
  - $(a + b) \ \mathbf{mod}\ m = \big((a \ \mathbf{mod}\ m) + (b \ \mathbf{mod}\ m)\big) \ \mathbf{mod}\ m$
  - $ab \ \mathbf{mod}\ m = \big((a \ \mathbf{mod}\ m)(b \ \mathbf{mod}\ m)\big) \ \mathbf{mod}\ m$

# Representasi Bilangan Bulat

# Representasi Bilangan Bulat

Diketahui $b$ bilangan bulat lebih besar dari 1. Jika $n$ adalah bilangan bulat positif, maka $n$ diekspresikan secara unik dalam bentuk:

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

untuk $k$ adalah bilangan bulat positif, $a_0, a_1, \ldots, a_k$ adalah bilangan bulat positif lebih kecil dari $b$ dan $a_k \neq 0$.

# Bilangan Desimal

- Bilangan basis 10
- 0, 1, 2, 3, 4, 5, 6, 7, 8, dan 9
- Contoh:

  $(987)_{10} = 987 = 9\times10^2 + 8\times10^1 + 7\times10^0$

# Bilangan Biner

- Bilangan basis 2
- 0 dan 1
- Contoh:

  $(101)_2 = 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = (5)_{10} = 5$

# Konversi Desimal ke Biner

- $(35)_{10} = (....)_2$

  35/2 = 17 sisa 1

  17/2 = 8 sisa 1

  8/2 = 4 sisa 0

  4/2 =2 sisa 0

  2/2 = 1 sisa 0

  1/2 = 0 sisa 1

**Bilangan biner yang didapat**
**Diambil dari bawah ke atas,**
**Yaitu: $(100011)_2$**

# Bilangan Oktal dan Heksadesimal

**Oktal**

- Bilangan basis 8
- 0, 1, 2, 3, 4, 5, 6, 7
- Oktal ke desimal
  - $(132)_8 = 1 \times 8^2 + 3 \times 8^1 + 2 \times 8^0$
    $= 64 + 24 + 2 = 90$
- Desimal ke oktal

  90 / 8 = 11 sisa 2
  11 / 8 = 1 sisa 3
  1 / 8 = 0 sisa 1

  132

**Heksadesimal**

- Bilangan basis 16
- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
- Heksa ke Desimal
  - $(ABC)_{16} = 10 \times 16^2 + 11 \times 16^1 + 12 \times 16^0$
    $= 2560 + 176 + 12 = 2748$
- Desimal ke heksa

  2748 / 16 = 171 sisa 12 (=C)
  171 / 16 = 10 sisa 11 (=B)
  10 / 16 = 0 sisa 10 (=A)

  ABC

# Algoritma Konversi Bilangan

- Konsep Konversi:

$$n = bq_0 + a_0, \qquad 0 \le a_0 < b$$
$$q_0 = bq_1 + a_1, \qquad 0 \le a_0 < b$$
$$\ldots$$
$$q_k = bq_{k+1} + a_k, \quad 0 \le a_k < b$$

Sampai $q_{k+1} = 0$

**ALGORITHM 1 Constructing Base $b$ Expansions.**

**procedure** *base b expansion*($n$, $b$: positive integers with $b > 1$)
$q := n$
$k := 0$
**while** $q \neq 0$
  $a_k := q$ **mod** $b$
  $q := q$ **div** $b$
  $k := k + 1$
**return** $(a_{k-1}, \ldots, a_1, a_0)$ $\{(a_{k-1} \ldots a_1 a_0)_b$ is the base $b$ expansion of $n\}$

# Algoritma Penjumlahan Bilangan Bulat

- Konsep Penjumlahan:

$$a = (a_{n-1}a_{n-2} \ldots a_1 a_0)_2$$
$$b = (b_{n-1}b_{n-2} \ldots b_1 b_0)_2$$

$$a_0 + b_0 = c_0 \cdot 2 + s_0,$$
$$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1,$$
$$\ldots$$
$$a_{n-1} + b_{n-1} + c_{n-2} = c_{n-1} \cdot 2 + s_{n-1},$$
$$s_n = c_{n-1}$$

Hasil = $(s_n s_{n-1} s_{n-2} \ldots s_1 s_0)_2$

**ALGORITHM 2 Addition of Integers.**

**procedure** *add*($a$, $b$: positive integers)
{the binary expansions of $a$ and $b$ are $(a_{n-1}a_{n-2} \ldots a_1a_0)_2$
  and $(b_{n-1}b_{n-2} \ldots b_1b_0)_2$, respectively}
$c := 0$
**for** $j := 0$ **to** $n - 1$
  $d := \lfloor (a_j + b_j + c)/2 \rfloor$
  $s_j := a_j + b_j + c - 2d$
  $c := d$
$s_n := c$
**return** $(s_0, s_1, \ldots, s_n)$ {the binary expansion of the sum is $(s_ns_{n-1} \ldots s_0)_2$}

# Contoh Penjumlahan Bilangan

$(1010)_2$

$(1100)_2$

-------------+

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

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

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

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

$1$

$(10110)_2$

$(726)_8$

$(123)_8$

-------------+

$6 + 3 = 1 \cdot 8 + 1$

$2 + 2 + 1 = 0 \cdot 8 + 5$

$7 + 1 + 0 = 1 \cdot 8 + 0$

$1$

$(1051)_8$

# Algoritma Perkalian Bilangan Bulat

- Konsep perkalian:

$$a = (a_{n-1}a_{n-2} \dots a_1 a_0)_2$$
$$b = (b_{n-1}b_{n-2} \dots b_1 b_0)_2$$

$$ab = a(b_0 2^0) + a(b_1 2^1) + \cdots + a(b_{n-1} 2^{n-1})$$

**ALGORITHM 3 Multiplication of Integers.**

**procedure** *multiply*($a$, $b$: positive integers)
{the binary expansions of $a$ and $b$ are $(a_{n-1}a_{n-2} \dots a_1a_0)_2$
  and $(b_{n-1}b_{n-2} \dots b_1b_0)_2$, respectively}
**for** $j := 0$ **to** $n - 1$
  **if** $b_j = 1$ **then** $c_j := a$ shifted $j$ places
  **else** $c_j := 0$
{$c_0, c_1, \dots, c_{n-1}$ are the partial products}
$p := 0$
**for** $j := 0$ **to** $n - 1$
  $p := add(p, c_j)$
**return** $p$ {$p$ is the value of $ab$}

# Contoh Perkalian Bilangan

$$
\begin{array}{r}
(1010)_2 \\
(\ \ 110)_2 \\
\text{-------------}\times \\
0000 \\
1010\ \\
1010\ \ \ \\
\text{-------------}+ \\
(111100)_2
\end{array}
$$

$$
\begin{array}{l}
\ \ (726)_8 \\
\ \ (\ \ 23)_8 \\
\text{-------------}\times \\
\ \ 2602 \\
1654 \\
\text{--------------}+ \\
(21342)_8
\end{array}
$$

$6 \times 3 = 18 \quad (> 7),$

$18 = 2 \cdot 8 + 2,$

jadi $6 \times 3 = {\color{red}2}2$

$2 \times 3 = 6, 6 + {\color{red}2} = 8 \quad (> 7),$

$8 = 1 \cdot 8 + 0$

jadi $2 \times 3 = {\color{red}1}0$

dst ...

# Algoritma DIV dan MOD untuk Bilangan Bulat

- Contoh: $a/d$

  $a = 11, d = 3$

  $q = 0, r = |a| = 11$
  - Loop 1:
    - $r = 11 - 3 = 8$
    - $q = 0 + 1 = 1$
  - Loop 2:
    - $r = 8 - 3 = 5$
    - $q = 1 + 1 = 2$
  - Loop 3:
    - $r = 5 - 3 = 2$
    - $q = 2 + 1 = 3$

**ALGORITHM 4 Computing div and mod.**

**procedure** *division algorithm*($a$: integer, $d$: positive integer)
$q := 0$
$r := |a|$
**while** $r \geq d$
    $r := r - d$
    $q := q + 1$
**if** $a < 0$ and $r > 0$ **then**
    $r := d - r$
    $q := -(q + 1)$
**return** $(q, r)$ {$q = a$ **div** $d$ is the quotient, $r = a$ **mod** $d$ is the remainder}

# Algoritma DIV dan MOD untuk Bilangan Bulat

- Contoh: $a/d$

  $a = -11, d = 3$

  $q = 0, r = |a| = 11$

  - Loop 1:
    - $r = 11 - 3 = 8$
    - $q = 0 + 1 = 1$
  - Loop 2:
    - $r = 8 - 3 = 5$
    - $q = 1 + 1 = 2$
  - Loop 3:
    - $r = 5 - 3 = 2$
    - $q = 2 + 1 = 3$
  - $r = 3 - 2 = 1$
  - $q = -(3 + 1) = -4$

**ALGORITHM 4 Computing div and mod.**

**procedure** *division algorithm*($a$: integer, $d$: positive integer)
$q := 0$
$r := |a|$
**while** $r \geq d$
    $r := r - d$
    $q := q + 1$
**if** $a < 0$ and $r > 0$ **then**
    $r := d - r$
    $q := -(q + 1)$
**return** $(q, r)$ $\{q = a$ **div** $d$ is the quotient, $r = a$ **mod** $d$ is the remainder$\}$

# Modular Exponentiation

- Menghitung
  $$b^n \mathbf{mod}\ m$$
- Konsep
  $$n = (a_{k-1}a_{k-2} \ldots a_1 a_0)_2$$
  $$b^n = b^{a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0}$$
  $$= b^{a_{k-1} \cdot 2^{k-1}} \cdot \ \ldots \cdot b^{a_1 \cdot 2} \cdot \ b^{a_0}$$

  Contoh: $3^{11}$
  $$11 = (1011)_2$$
  $$3^{11} = 3^{1 \cdot 8} \cdot 3^{0 \cdot 4} \cdot 3^{1 \cdot 2} \cdot \ 3^1$$
  $$= 3^8 \cdot 3^0 \cdot 3^2 \cdot \ 3^1$$
  $$= 6561 \cdot 1 \cdot 9 \cdot \ 3 = 177147$$

**ALGORITHM 5 Fast Modular Exponentiation.**

**procedure** *modular exponentiation*($b$: integer, $n = (a_{k-1}a_{k-2} \ldots a_1 a_0)_2$,
    $m$: positive integers)
$x := 1$
$power := b$ **mod** $m$
**for** $i := 0$ **to** $k - 1$
    **if** $a_i = 1$ **then** $x := (x \cdot power)$ **mod** $m$
    $power := (power \cdot power)$ **mod** $m$
**return** $x\{x$ equals $b^n$ **mod** $m\}$

# Modular Exponentiation

- Contoh: $3^{11}$ **mod** 13

  $11 = (1011)_2, x = 1,$
  $power = 3 \textbf{ mod } 13 = 3$

  $a_0 = 1, x = (1 \cdot 3) \textbf{ mod } 13 = 3,$
  $power = 3 \cdot 3 \textbf{ mod } 13$
  $= 3^2 \textbf{ mod } 13$
  $= 9 \textbf{ mod } 13$
  $= 9$

  $a_1 = 1, x = (3 \cdot 9) \textbf{ mod } 13 = 1,$
  $power = 81 \textbf{ mod } 13 = 3$

  $a_2 = 0, x = 1,$
  $power = 9 \textbf{ mod } 13 = 9$

  $a_3 = 1, x = (1 \cdot 9) \textbf{ mod } 13 = 9,$
  $power = 81 \textbf{ mod } 13 = 3$

  Jadi, $3^{11} \textbf{ mod } 13 = 3$

**ALGORITHM 5 Fast Modular Exponentiation.**

**procedure** *modular exponentiation*($b$: integer, $n = (a_{k-1}a_{k-2} \dots a_1a_0)_2$,
    $m$: positive integers)
$x := 1$
$power := b \textbf{ mod } m$
**for** $i := 0$ **to** $k - 1$
    **if** $a_i = 1$ **then** $x := (x \cdot power) \textbf{ mod } m$
    $power := (power \cdot power) \textbf{ mod } m$
**return** $x$ {$x$ equals $b^n \textbf{ mod } m$}

# Bilangan Prima dan Greatest Common Divisor

# Bilangan Prima

- Sebuah bilangan bulat $p$ disebut sebagai **bilangan prima** jika dan hanya jika terdapat **hanya dua faktor** dari $p$, yaitu **1 dan $\boldsymbol{p}$** itu sendiri.
- Sebuah bilangan bulat positif yang **lebih dari satu dan bukan bilangan prima** disebut **bilangan komposit**.
- Contoh: tentukan apakah 7 dan 9 bilangan prima atau komposit
  - 7 adalah bilangan prima karena hanya bisa dibagi habis oleh 1 dan 7
  - 9 adalah bilangan komposit karena bisa dibagi habis oleh 3

# Faktorisasi Bilangan Prima

- Faktorisasi bilangan prima dari 100
  - $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- Jika $n$ adalah bilangan bulat komposit, maka $n$ memiliki faktor (pembagi) sebuah bilangan prima lebih kecil atau sama dengan $\sqrt{n}$
  - Tunjukkan bahwa 101 adalah bilangan prima
    - Bilangan prima dari $\sqrt{101}$ adalah 2, 3, 5, 7.
    - 101 tidak bisa dibagi habis oleh 2, 3, 5, 7
    - 101 adalah bilangan prima
- Faktorisasi bilangan prima dari 7007:
  - 2, 3, 4, 5 tidak bisa membagi habis 7007
  - 7 bisa membagi habis 7007: 7007/7 = 1001
  - 1001 bisa dibagi habis dengan 7: 1001/7 = 143
  - 143 tidak bisa dibagi habis dengan 7 tapi 11 bisa: 143/11 = 13
  - 13 adalah bilangan prima
  - Faktorisasi dari $7007 = 7^2 \cdot 11 \cdot 13$

# Greatest Common Divisors (GCD)

Faktor Persekutuan terBesar (FPB)

- $\mathrm{GCD}(a, b)$: bilangan terbesar yang membagi habis $a$ dan $b$, untuk $a \neq 0$ dan $b \neq 0$ adalah bilangan bulat
  - $\mathrm{GCD}(24{,}36) = 12$
  - $\mathrm{GCD}(17{,}22) = 1$
- Bilangan bulat $a$ dan $b$ disebut *relatively prime*, jika $\mathrm{GCD}(a, b) = 1$
- Deretan bilangan bulat $a_1, a_2, \ldots a_n$ disebut *pairwise relatively prime* jika $\mathrm{GCD}\left(a_i, a_j\right) = 1$, untuk $1 \leq i < j \leq n$.
  - 10, 17, 21 adalah *pairwise relatively prime* karena $\mathrm{GCD}(10{,}17) = 1$, $\mathrm{GCD}(17{,}21) = 1$, dan $\mathrm{GCD}(10{,}21) = 1$
  - 10, 19, 24 bukan *pairwise relatively prime* karena $\mathrm{GCD}(10{,}24) = 2$

# Least Common Multiples (LCM)

Kelipatan Persekutuan terKecil (KPK)

- $\mathrm{lcm}(a, b)$: bilangan terkecil habis dibagi oleh $a$ dan $b$, untuk $a$ dan $b$ adalah bilangan bulat positif.
  - $\mathrm{lcm}(12,18) = 36$
  - $\mathrm{lcm}(24,36) = 72$

# Faktorisasi Bilangan Prima untuk GCD dan LCM

- $\text{GCD}(168,180)$
  - $168 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 = 2^3 \cdot 3 \cdot 7$
  - $180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^2 \cdot 5$
  - $\text{GCD}(168,180) = 2^{\min(3,2)} 3^{\min(1,2)} 7^{\min(1,0)} 5^{\min(0,1)} = 2^2 \cdot 3 = 12$
- $\text{lcm}(45,75)$
  - $45 = 3^2 \cdot 5$
  - $75 = 3 \cdot 5^2$
  - $\text{lcm}(45,75) = 3^{\max(2,1)} 5^{\max(1,2)} = 3^2 \cdot 5^2 = 225$

# Algoritma Euclidean

- Menggunakan faktorisasi bilangan prima tidak efisien
- Konsep: $\mathrm{GCD}(287, 91)$

$$287 = 3 \cdot 91 + 14$$
$$91 = 6 \cdot 14 + 7$$
$$14 = 2 \cdot 7 + 0$$
$$\mathrm{GCD}(287,91) = 7$$

**ALGORITHM 1 The Euclidean Algorithm.**

**procedure** $gcd(a, b$: positive integers)
$x := a$
$y := b$
**while** $y \neq 0$
    $r := x$ **mod** $y$
    $x := y$
    $y := r$
**return** $x\{\text{gcd}(a, b) \text{ is } x\}$

# GCD sebagai Kombinasi Linier

- Jika $a$ dan $b$ adalah bilangan bulat positif, maka terdapat bilangan bulat $s$ dan $t$ sehingga $\mathrm{GCD}(a,b) = sa + tb$
- Contoh: $\mathrm{GCD}(287, 91)$

  $287 = 3 \cdot 91 + 14$

  $91 = 6 \cdot 14 + 7$

  $14 = 2 \cdot 7 + 0$
- Extended Euclidean untuk menentukan nilai $s$ dan $t$

  $91 = 6 \cdot 14 + 7 \quad \rightarrow \quad 7 = 91 - 6 \cdot 14$

  $287 = 3 \cdot 91 + 14 \quad \rightarrow \quad 14 = 287 - 3 \cdot 91$

  $7 = 91 - 6 \cdot 14 \quad \rightarrow \quad 7 = 91 - 6 \cdot (287 - 3 \cdot 91) = 19 \cdot 91 - 6 \cdot 287$

  Jadi, $s = -6$ dan $t = 19$

# Kongruensi dan Penyelesaiannya

# Kongruensi

- $a \equiv b (\mathrm{mod}\ m)$ jika dan hanya jika $a \bmod m = b \bmod m$
  - Contoh: apakah $14 \equiv 8 (\mathrm{mod}\ 6)$?
    - Iya, karena $14 \bmod 6 = 8 \bmod 6$ ➔ $2 = 2$
- Jika $m$ bilangan bulat positif dan $a, b, c$ adalah bilangan bulat. Jika $ac \equiv bc (\mathrm{mod}\ m)$ dan $\mathrm{GCD}(c, m) = 1$, maka $a \equiv b (\mathrm{mod}\ m)$
  - $c$ adalah relatively prime dengan $m$
  - $m \mid a - b$

# Kongruensi Linier (1)

- $ax \equiv b (\text{mod } m)$, untuk $m$ bilangan bulat positif, $a$ dan $b$ adalah bilangan bulat, dan $x$ adalah peubah.
  - Bagaimana mencari semua nilai $x$ yang memenuhi kongruensi $ax \equiv b (\text{mod } m)$?
  - **Inverse dari $\boldsymbol{a}$ modulo $\boldsymbol{m}$**, $\bar{a}a \equiv 1 (\text{mod } m)$, untuk $a$ dan $m$ adalah *relatively prime*.
    - $\bar{a}$ disebut inverse perkalian
    - Gunakan persamaan euclidean untuk mencari $\text{GCD}(a, m) = 1$, yaitu $m = k \cdot a + 1$, dilanjutkan dengan extended euclidean
- Contoh: tentukan inverse dari 3 modulo 7

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

  maka $-2$ adalah inverse dari 3 modulo 7

  Selain itu, $(-2 + 7) = 5$ dan 12 juga termasuk dari inverse dari 3 modulo 7

# Kongruensi Linier (2)

- Solusi untuk $3x \equiv 4 (\mathrm{mod}\ 7)$

  Inverse dari 3 modulo 7 adalah $-2$

  $-2 \cdot 3 = -6 \equiv 1 (\mathrm{mod}\ 7)$

  $-2 \cdot 3x \equiv -2 \cdot 4 (\mathrm{mod}\ 7)$

  $x \equiv -8 (\mathrm{mod}\ 7)$

  $x \bmod 7 = -8 \bmod 7$

  $x \bmod 7 = 6$

  $x \equiv 6 (\mathrm{mod}\ 7)$

  Untuk $x = 6$, maka $3 \cdot 6 = 18 \equiv 4 (\mathrm{mod}\ 7)$

  Solusi lainnya untuk $x$ adalah $6 + 7 = 13, 20, \ldots$ dan $-1, -8, -15, \ldots$

https://www.math.uh.edu/~pwalker/3336Sp21Sec4.4Slides.pdf

# Contoh Inverse $a$ Modulo $m$

- Inverse 55 modulo 7

  <u>Euclidean:</u>

  $55 = 7 \cdot 7 + 6$ ➔ $6 = 55 - 7 \cdot 7$

  $7 = 1 \cdot 6 + 1$ ➔ $1 = 7 - 1 \cdot 6$

  <u>Extended Euclidean:</u>

  $1 = 7 - 1 \cdot (55 - 7 \cdot 7)$

  $1 = 8 \cdot 7 - 1 \cdot 55$

  Inverse 55 modulo 7 $= -1$,

  atau nilai positifnya $(-1 + 7) = 6$

  Inverse 55 modulo 7 $= 6$

- Inverse 7 modulo 31

  <u>Euclidean:</u>

  $31 = 4 \cdot 7 + 3$ ➔ $3 = 31 - 4 \cdot 7$

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

  <u>Extended Euclidean:</u>

  $1 = 7 - 2 \cdot (31 - 4 \cdot 7)$

  $1 = 9 \cdot 7 - 2 \cdot 31$

  Inverse 7 modulo 31 $= 9$

# Sistem Kongruensi Linier

**Chinese remainder theorem**: diketahui deretan bilangan bulat positif $m_1, m_2, \ldots, m_n$ adalah *pairwise relatively prime* yang lebih besar dari satu dan deretan bilangan bulat sembarang $a_1, a_2, \ldots, a_n$. Maka sistem:

$$\begin{gathered} x \equiv a_1 (\mathrm{mod}\, m_1) \\ x \equiv a_2 (\mathrm{mod}\, m_2) \\ \vdots \\ x \equiv a_n (\mathrm{mod}\, m_n) \end{gathered}$$

memiliki solusi modulo unik $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

-------------------

$x \equiv a_k M_k y_k \equiv a_k (\mathrm{mod}\, m_k)$ untuk $M_k = m/m_k$

$y_k$ adalah inverse of $M_k$ modulo $m_k$

# Contoh

- Diketahui sistem kongruensi linier berikut:

$$x \equiv 2 (\mathrm{mod}\ 3)$$
$$x \equiv 3 (\mathrm{mod}\ 5)$$
$$x \equiv 2 (\mathrm{mod}\ 7)$$

- $x \equiv a_k M_k y_k = a_k (\mathrm{mod}\ m_k)$
  - $m = 3 \cdot 5 \cdot 7 = 105$
  - $M_1 = \frac{105}{3} = 35, M_2 = \frac{105}{5} = 21, M_3 = \frac{105}{7} = 15$
  - $M_1 = 35 \equiv 2 (\mathrm{mod}\ 3)$, inverse dari 35 modulo 3 adalah $y_1 = 2$
  - $M_2 = 21 \equiv 3 (\mathrm{mod}\ 5)$, inverse dari 21 modulo 5 adalah $y_2 = 1$
  - $M_3 = 15 \equiv 2 (\mathrm{mod}\ 7)$, inverse dari 15 modulo 7 adalah $y_3 = 1$
  - $a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$
    $= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$
    $= 233 \equiv 23 (\mathrm{mod}\ 105)$
- $\boldsymbol{x = 23}$

- Inverse 35 modulo 3:

  Euclidean:
  $35 = 11 \cdot 3 + 2$ ➔ $2 = 35 - 11 \cdot 3$
  $3 = 1 \cdot 2 + 1$ ➔ $1 = 3 - 1 \cdot 2$
  Extended Euclidean:
  $1 = 3 - 1 \cdot (35 - 11 \cdot 3) = 12 \cdot 3 - 1 \cdot 35$
  Fokus ke konstants dari 35, yaitu -1 yang merupakan inverse 35 modulo 3.
  Kita bisa menentukan nilai positif untuk inverse tersebut yaitu $(-1 + 3) = 2$
- Dengan cara yang sama, lakukan perhitungan untuk Inverse 21 modulo 5, dan 15 modulo 7

# Fermat’s Little Theorem

- Jika $p$ adalah bilangan prima dan $a$ adalah bilangan bulat tidak dapat dibagi habis oleh $p$, maka $a^{p-1} \equiv 1 \pmod{p}$.
- Untuk setiap $a$ adalah bilangan bulat, $a^p \equiv a \pmod{p}$.
- Contoh: $7^{222} \bmod 11$
  - $7^{11-1} = 7^{10} \equiv 1 \pmod{41}$
  - $222$ dibagi $10$ ➔ $222 = 10 \cdot 22 + 2$
  - $7^{222} = 7^{10 \cdot 22+2} = (7^{10})^{22} 7^2$
  - $(7^{10})^{22} 7^2 \bmod 11 = \left(\left((7^{10})^{22} \bmod 11\right)(7^2 \bmod 11)\right) \bmod 11$
    $= \left((1)^{22} \cdot 49\right) \bmod 11 = 5$
  - $7^{222} \bmod 11 = 5$

# Latihan Soal

# Latihan Soal 1

1. Jawablah pertanyaan berikut dengan memberikan proses atau perhitungan secara rinci:
   a. Jelaskan apakah 17 dapat membagi habis 357 dan 1001!
   b. Diketahui $a \equiv -133 (\mathrm{mod}\ 23)$ dan $b \equiv 261 (\mathrm{mod}\ 23)$. Tentukan hasil dari $(a + b)\ \mathrm{mod}\ 23$!

# Latihan Soal 2

2. Berikan secara rinci proses berikut ini:
   a. Konversi bilangan desimal 1025 ke bilangan biner, oktal dan heksadesimal!
   b. Tentukan hasil penjumlahan dan perkalian dari pasangan bilangan basis 3 $(12021)_3$ dan $(2112)_3$:

# Latihan Soal 3

3. Jelaskan cara untuk menentukan:
   a. apakah $107$ dan $114$ adalah bilangan prima
   b. $\text{GCD}(124,323)$ dan ekpresinya dalam bentuk kombinasi linier

# Latihan Soal 4

4. Secara rinci, selesaikan kongruensi linier $2x \equiv 7(\text{mod } 17)$ menggunakan inverse of 2 modulo 17.

# Jawaban Latihan Soal 5

5. Tuliskan proses pencarian solusi (nilai  untuk $x$) sistem kongruensi liner berikut:

$$x \equiv 2 (\text{mod } 3)$$
$$x \equiv 1 (\text{mod } 4)$$
$$x \equiv 3 (\text{mod } 5)$$

# Latihan Soal 6

6. Tuliskan proses pencarian hasil dari $23^{1002} \bmod 41$: