Bilangan Prima

Definisi

- Definisi

> Suatu bilangan bulat $p > 1$ disebut bilangan prima jika hanya p memiliki dua faktor positif yaitu 1 dan p
>
> Bilangan bulat positif yang lebih besar dari 1 dan bukan prima disebut bilangan komposit

- Suatu bilangan bulat n adalah bilangan komposit jika dan hanya jika terdapat suatu bilangan bulat a sehingga $a \mid n$ dan $1 < a < n$

Teorema Dasar Aritmetika

- Teorema

> Setiap bilangan bulat positif dapat ditulis secara unik sebagai sebuah bilangan prima atau perkalian dari dua atau lebih faktor prima di mana faktor-faktor prima tersebut dituliskan dalam urutan yang tidak menurun

- Konsekuensi: setiap bilangan positif pasti memiliki faktor prima
- Contoh faktorisasi prima
  - $128 = 2 . 2 . 2 . 2 . 2 . 2 . 2 = 2^7$
  - $641 = 641$
  - $999 = 3 . 3 . 3 . 37 = 3^3 . 37$

Pembagi Prima dari Bilangan Komposit
Trial Division

- Teorema

Jika n suatu bilangan komposit, maka n memiliki sebuah pembagi prima yang kurang dari atau sama dengan $\sqrt{n}$

Pembagi Prima dari Bilangan Komposit

Trial Division

- Bukti
  - Jika n komposit, maka n memiliki sebuah faktor a di mana $1 < a < n$. Jadi, $n = ab$ di mana a dan b bilangan bulat positif yang lebih dari 1
  - Perhatikan bahwa $a \leq \sqrt{n}$ atau $b \leq \sqrt{n}$, karena kalau tidak, $ab > \sqrt{n} \cdot \sqrt{n} = n$
  - Dengan demikian, n memiliki pembagi positif yang tidak melebihi $\sqrt{n}$
  - Pembagi positif ini adalah bilangan prima atau jika bukan, maka menurut teori dasar aritmetika, pembagi positif tersebut haruslah memiliki pembagi prima juga
  - Dalam kedua kasus, n selalu punya pembagi prima yang kurang atau sama dengan $\sqrt{n}$

Pembagi Prima dari Bilangan Komposit
Trial Division

Contoh

- Apakah 101 merupakan bilangan prima?
  - Perhatikan bahwa bilangan prima yang kurang dari $\sqrt{101}$ adalah 2, 3, 5, dan 7
  - Dengan memeriksa satu per satu kita dapat memperoleh bahwa tidak ada satu pun dari bilangan-bilangan prima tersebut yang habis membagi 101
  - Jadi, bilangan 101 seharusnya adalah bilangan prima

Pembagi Prima dari Bilangan Komposit

<u>Contoh</u>

- Hitunglah faktorisasi prima dari 7007
  - Jawabannya: 7007 = 7 . 7 . 11 . 13 = 7^2 . 11. 13
  - Bagaimana memperolehnya?
    - Gunakan pohon faktor atau
    - Carilah sesuai dengan petunjuk teorema dasar sebelumnya

Banyaknya Bilangan Prima yang Ada

- Teorema

> Banyaknya bilangan prima adalah tidak berhingga

- Euclid's Proof – menggunakan kontradiksi
  - Asumsikan jumlah bilangan prima berhingga: $p_1, p_2, \dots, p_n$
  - Ambil bilangan $N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$
  - Terlihat bahwa N tidak habis dibagi p_1, p_2, ..., maupun p_n
  - Dengan demikian, N mungkin prima atau N habis dibagi bilangan prima lain yang tidak ada di p_1 hingga p_n
  - Terbukti bahwa banyaknya bilangan prima adalah tak berhingga

Greatest Common Divisor (GCD)

Greatest Common Divisor (GCD)

Faktor Persekutuan Terbesar (FPB)

- Definisi

> Misalkan ***a*** dan ***b*** bilangan bulat di mana setidaknya salah satunya bukan 0, maka bilangan bulat terbesar ***d*** yang memenuhi ***d* | *a*** dan ***d* | *b*** disebut *greatest common divisor* (gcd) dari ***a*** dan ***b*** dan ditulis **gcd(*a*,*b*)**

Greatest Common Divisor (GCD)

Faktor Persekutuan Terbesar (FPB)

- Contoh
  - Berapakah gcd(24, 36)?
    - gcd(24, 36) = 12
  - Berapakah gcd(17, 25)?
    - gcd(17, 25) = 1
  - Berapakah gcd(120, 500)?
    - gcd(120, 500) = ?

Greatest Common Divisor (GCD)

Faktor Persekutuan Terbesar (FPB)

- Teorema

> Misalkan ***a*** dan ***b*** bilangan bulat bukan nol dengan faktorisasi prima $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ dan $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ di mana ***a_i, b_i*** bilangan bulat non negatif, maka:
>
> $$\gcd(a, b) = p_1^{min(a_1, b_1)} p_2^{min(a_2, b_2)} \cdots p_n^{min(a_n, b_n)}$$

Greatest Common Divisor (GCD)

Faktor Persekutuan Terbesar (FPB)

- Contoh
  - Berapakah gcd(120, 500)?
    - $120 = 2^3 . 3 . 5$
    - $500 = 2^2 . 5^3$
    - $\gcd(120, 500) = 2^{\min(3,2)} . 3^{\min(1,0)} . 5^{\min(1,3)}$
    - $\gcd(120, 500) = 2^2 . 3^0 . 5^1 = 20$
  - Berapakah gcd(212, 365)?
    - ?

Relatif Prima

- Definisi

> Bilangan bulat ***a*** dan ***b*** dikatakan **relatif prima** jika **gcd(*a*, *b*) = 1**.
>
> Bilangan-bilangan bulat $a_1, a_2, \ldots, a_n$ dikatakan ***pairwise relatively prime*** jika $\gcd(a_i, a_j) = 1$ untuk setiap $1 \leq i < j \leq n$.

Relatif Prima

- Contoh
  - Apakah 10, 17, dan 21 merupakan bilangan-bilangan yang *pairwise relatively prime*?
    - gcd(10, 17) = 1
    - gcd(10, 21) = 1
    - gcd(17, 21) = 1
    - Semua gcd dari pasangan bilangan yang memenuhi syarat adalah 1
    - Dengan demikian 10, 17, dan 21 merupakan bilangan-bilangan yang *pairwise relatively prime*

Relatif Prima

- Contoh
  - Apakah 10, 19, dan 24 merupakan bilangan-bilangan yang *pairwise relatively prime*?
    - Cari gcd(10, 19) = ?
    - Cari gcd(10, 24) = ?
    - Cari gcd(19, 24) = ?
    - Apakah semua gcd dari pasangan bilangan yang memenuhi syarat adalah 1?
  - Apakah 12, 17, 35, dan 42 merupakan bilangan-bilangan yang *pairwise relatively prime*?
    - ?

Least Common Multiple (LCM)

Kelipatan Persekutuan Terkecil (KPK)

- Definisi

> *Least common multiple* dari dua bilangan bulat positif ***a*** dan ***b*** (ditulis lcm(a, b)) adalah bilangan bulat positif terkecil yang sama-sama habis dibagi oleh ***a*** dan ***b***

Least Common Multiple (LCM)
Kelipatan Persekutuan Terkecil (KPK)

- Contoh
  - Berapakah lcm(10, 12)?
    - lcm(10, 12) = 60
  - Berapakah lcm(24, 36)?
    - lcm(24, 36) = 72
  - Berapakah lcm(120, 500)?
    - lcm(120, 500) = ?

Least Common Multiple (LCM)

Kelipatan Persekutuan Terkecil (KPK)

- Teorema

Misalkan ***a*** dan ***b*** bilangan bulat bukan nol dengan faktorisasi prima $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ dan $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ di mana $\boldsymbol{a_i}$, $\boldsymbol{b_i}$ bilangan bulat non negatif, maka:

$$\mathrm{lcm}(a, b) = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \dots p_n^{max(a_n,b_n)}$$

Least Common Multiple (LCM)
Kelipatan Persekutuan Terkecil (KPK)

- Contoh
  - Berapakah lcm(120, 500)?
    - $120 = 2^3 . 3 . 5$
    - $500 = 2^2 . 5^3$
    - $\text{lcm}(120, 500) = 2^{\max(3,2)} . 3^{\max(1,0)} . 5^{\max(1,3)}$
    - $\text{lcm}(120, 500) = 2^3 . 3^1 . 5^3 = 3000$
  - Berapakah lcm(212, 365)?
    - ?

Hubungan GCD dan LCM

- Teorema

Misalkan ***a*** dan ***b*** adalah bilangan bulat positif maka: ***ab* = gcd(*a*, *b*) . lcm(*a*, *b*)**

- Contoh
  - 120 . 500 = gcd(120, 500) . lcm(120, 500)
    = 20 . 3000
    = 60000

Mencari GCD dengan Algoritma Euclidean

- Contoh
  - Berapakah gcd(91, 287)?
    - Perhatikan:

$$a = b \, . \, q + r$$

$$\mathbf{287 = 91 \, . \, 3 + 14}$$

$$\mathbf{91 = 14 \, . \, 6 + 7}$$

$$\mathbf{14 = 7 \, . \, 2 + 0}$$

    - Jadi, **gcd(91, 287) = 7**

Algoritma Euclidean

```
procedure : gcd(a, b: positive integer)
     x := a
     y := b
     while y ≠ 0
     begin
          r := x mod y
          x := y
          y := r
     end {gcd(a, b) is x}
```

Ilustrasi debugging

a = 287 b = 91

x = y . q + r

287 = 91 . 3 + 14

91 = 14 . 6 + 7

14 = 7 . 2 + 0

7 = 0 ...

Sampai di sini maka:

x = 7 dan y = 0

Sehingga:

return x sebagai GCD (a,b)

Algoritma Euclidean

- Teorema

Misalkan ***a* = *bq* + *r***, di mana ***a***, ***b***, ***q***, dan ***r*** adalah bilangan bulat maka berlaku:

gcd(*a*, *b*) = gcd(*b*, *r*)

atau

gcd(*a*, *b*) = gcd(*b*, *a mod b*)

Perhatikan contoh sebelumnya:

gcd(91, 287) = gcd(91, 14) = gcd(14, 7) = gcd(7, 0) = 7

Algoritma Euclidean

- Bukti
  - Cukup dibuktikan bahwa untuk setiap bilangan bulat ***d*** maka ***d* | *a*** dan ***d* | *b*** jika dan hanya jika ***d* | *b*** dan ***d* | *r***
  - Berarti:
    - Buktikan jika ***d* | *a*** dan ***d* | *b*** maka ***d*** | ***r***
    - Sebaliknya, buktikan jika ***d* | *b*** dan ***d* | *r*** maka ***d* | *a***

Algoritma Euclidean

- Bukti (lanjutan)
  - Pertama: jika $d \mid a$ dan $d \mid b$ maka $d \mid r$
    - Jika $d \mid a$ dan $d \mid b$ maka $a = md$ dan $b = nd$ untuk suatu bilangan bulat m dan n
    - Perhatikan bahwa $a = bq + r$ sama saja $r = a - bq$
    - Melalui substitusi kita mendapatkan:

      $$r = md - ndq = (m - nq)d$$
    - Perhatikan bahwa bentuk di atas jelas menunjukkan bahwa $d \mid r$

Algoritma Euclidean

- Bukti (lanjutan)
  - Sebaliknya: jika $d \mid b$ dan $d \mid r$ maka $d \mid a$
    - Jika $d \mid b$ dan $d \mid r$ maka $b = md$ dan $r = nd$ untuk suatu bilangan bulat m dan n
    - Perhatikan bahwa $a = bq + r$
    - Melalui substitusi kita mendapatkan:

      $a = mdq + nd = (mq + n)d$
    - Perhatikan bahwa bentuk di atas jelas menunjukkan bahwa $d \mid a$

Latihan Menghitung GCD dengan Algoritma Euclidean

- Berapakah gcd(240, 139)?
- Berapakah gcd(414, 662)?
- Berapakah gcd(252, 198)?

GCD Sebagai Kombinasi Linear Bilangan

- Teorema (Bezout's Theorem)

Jika a dan b bilangan bulat positif, maka terdapat bilangan bulat s dan t sehingga
gcd(a, b) = $sa + tb$

GCD Sebagai Kombinasi Linear Bilangan

- Nyatakan gcd(252, 198) sebagai kombinasi linear 252 dan 198!
- Bagaimana mencari ***s*** dan ***t***?
  - Cari gcd(252, 198) terlebih dahulu dengan Euclidean:

    252 = 198 . 1 + 54

    198 = 54 . 3 + 36

    54 = 36 . 1 + 18

    36 = **18** . 2 + 0

    - Jadi, gcd(252, 198) = 18

GCD Sebagai Kombinasi Linear Bilangan

Bagaimana mencari ***s*** dan ***t***? Proses pencarian gcd tersebut selanjutnya dapat dibalik

Pencarian GCD dengan Euclidean tadi:

$$
\begin{aligned}
252 &= 198 \cdot 1 + 54 \\
198 &= 54 \cdot 3 + 36 \\
54 &= 36 \cdot 1 + 18 \\
36 &= \mathbf{18} \cdot 2 + 0
\end{aligned}
$$

$$
\begin{aligned}
18 &= 54 - 36 \cdot 1 \\
&= 54 - (198 - 54 \cdot 3) \\
&= 54 \cdot 4 - 198 \\
&= (252 - 198) \cdot 4 - 198 \\
&= 252 \cdot 4 - 198 \cdot 5
\end{aligned}
$$

Jadi, $\gcd(252, 198) = \mathbf{4} \cdot 252 \mathbf{-} \mathbf{5} \cdot 198$