3.1 TEOREMA DASAR ARITMATIKA

Definisi 3.1

Suatu bilangan bulat $p > 1$ disebut (bilangan) prima, jika pembagi positif bilangan tersebut hanya 1 dan p. Jika bilangan bulat lebih dari satu bukan bilangan prima disebut (bilangan) komposit.

Teorema 3.1
Jika p bilangan prima dan $p \mid ab$, maka $p \mid a$ atau $p \mid b$.

Bukti:
Jika $p \mid a$, maka pernyataan di atas benar.
Misalkan $p \nmid a$, karena p prima (pembagi dari p hanya p dan satu) maka gcd (p,a) = 1.
Karena $p \mid ab$ dan gcd (p,a) = 1 menurut lemma Euclid disimpulkan $p \mid b$.

Corollary 1.
Jika p prima dan $p \mid a_1a_2...a_n$, maka $p \mid a_k$ untuk suatu k dengan $1 \leq k \leq n$

Bukti:
Akan dibuktikan melalui induksi matematika
Untuk n = 1 benar karena untuk p prima dan $p \mid a_1$, maka $p \mid a_k$ $1 \leq k \leq 1$.
Untuk n = 2 benar seperti telah dibuktikan pada teorema 3.1.
Misalkan untuk n > 2 benar. Artinya jika p membagi suatu hasil perkalian dari faktor-faktor yang banyaknya kurang dari n, maka p membagi paling sedikit sebuah faktor.
Misalkan $p \mid a_1a_2...a_n$, berdasarkan teorema 3.1. maka $p \mid a_1a_2...a_{n-1}$ atau $p \mid a_n$.
Jika $p \mid a_n$ kita selesai. Jika $p \mid a_1a_2...a_{n-1}$, maka menurut pemisalan maka $p \mid a_k$ suatu k dengan $1 \leq k \leq n-1$
Jadi disimpulkan, jika p prima dan $p \mid a_1a_2...a_n$, maka $p \mid a_k$ untuk suatu k dengan $1 \leq k \leq n$.

Corollary 2.
Jika $p, q_1, q_2, ..., q_n$ semuanya prima dan $p \mid q_1q_2...,q_n$, maka $p = q_k$ untuk suatu k dengan $1 \leq k \leq n$,

Bukti:
Jika p prima dan $p \mid q_1q_2...,q_n$, berdasarkan corollary 1 disimpulkan $p \mid q_k$ untuk suatu k dengan $1 \leq k \leq n$.
Karena q_k prima, maka q_k hanya memiliki pembagi positif 1 dan q_k
Jadi $p = 1$ atau $p = q_k$. Karena $p > 1$ disimpulkan $p = q_k$.

Teorema 3.2 (Teorema Dasar Aritmatika)
Setiap bilangan bulat positif n > 1 dapat dinyatakan sebagai suatu perkalian bilangan-bilangan prima, dan representasi tersebut unik.

Bukti:
Bilangan bulat n > 1 adalah prima atau komposit.
Jika n prima tidak ada hal yang harus dibuktikan lagi.
Jika n komposit, maka ada bilangan bulat d $\mid$ n dengan 1 < d < n.
Menurut WOP ada bilangan bulat terkecil diantara bilangan bulat d dan misalkan p_1.
Maka p_1 haruslah bilangan prima.
Karena jika p_1 bukan bilangan prima, maka ada q dimana
$1 < q < p_1$ dengan $q \mid p_1$ dan $p_1 \mid n$ sehingga $q \mid n$. Hal ini bertentangan dengan p_1 pembagi n yang terkecil yang besar 1.
Dengan demikian dapat kita tulis $n = p_1 n_1$ dimana p_1 prima dan
$1 < n_1 < n$.
Jika n_1 prima, maka kita peroleh ekspresi $n = p_1 n_1$ yang kita inginkan.
Jika n_1 bukan prima, dengan prosedur seperti di atas diperoleh bilangan prima yang kedua yaitu p_2 yang memenuhi $n_1 = p_2 n_2$, sehingga $n = p_1 p_2 n_2$ dengan $1 < n_2 < n_1$.
Jika n_2 prima maka tidak perlu dilanjutkan.
Jika n_2 bukan prima, maka diperoleh bilangan prima yang ketiga yaitu p_3 dengan $n_2 = p_3 m_3$ dan $n = p_1 p_2 p_3 n_3$ dimana $1 < n_3 < n_2$.

Barisan turun $n > n_1 > n_2 > ... > 1$ adalah barisan terhingga, oleh karena itu setelah sejumlah langkah yang berhingga, n_{k-1} adalah sebuah bilangan prima, sebut saja p_k. Ini menyatakan faktorisasi prima $n = p_1 p_2 ... p_k$.

Untuk membuktikan keunikan faktorisasi prima, misalkan n dapat diekspresikan sebagai perkalian bilangan-bilangan prima dengan dua cara yaitu
$n = p_1 p_2 ... p_r = q_1 q_2 ... q_s$ dengan $r \le s$ dimana p_i dan q_j semua bilangan prima dan dalam besaran yang naik dapat ditulis
$p_1 \le p_2 \le ... \le p_r$; $q_1 \le q_2 \le ... \le q_s$
Karena $p_1 \mid n = q_1 q_2 ... q_s$, berdasarkan corollary 2 teorema 3.1
$p_1 = q_k$ untuk suatu k; dan $p_1 \ge q_1$.
Dengan penalaran yang sama, karena $q_1 \mid n = p_1 p_2 ... p_r$, berdasarkan corollary 2 teorema 3.1 $q_1 = p_k$ untuk suatu k; dan $q_1 \ge p_1$.
Dari $p_1 \ge q_1$ dan $q_1 \ge p_1$ disimpulkan $p_1 = q_1$, sehingga diperoleh
$p_2 p_3 ... p_r = q_2 q_3 ... q_s$
Dengan mengulang prosedur yang sama seperti di atas diperoleh
$p_2 = q_2$ dan $p_3 p_4 ... p_r = q_3 q_4 ... q_s$.
Andaikan r < s dan proses di atas diteruskan akan sampai pada
$1 = q_{r+1} q_{r+2} ... q_s$. Hal ini tidak mungkin karena $q_j > 1$, jadi haruslah
r = s dan $p_1 = q_1$, $p_2 = q_2$, ..., $p_r = q_s$. Artinya faktorisasi prima dari n adalah unik.

Corollary
Setiap bilangan bulat n > 1 dapat dituliskan secara unik dalam bentuk kanonik yaitu
$n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ untuk i = 1, 2, ... r, k_i bilangan bulat positif dan p_i bilangan prima dengan $p_1 < p_2 < ... < p_r$.
Bukti:

$n = p_1 p_2 ... p_r$ dengan $p_1 \leq p_2 \leq ... \leq p_r$ dengan demikian dapat terjadi $p_1 = p_2$ sehingga $n = p_1^2 p_3 ... p_r$ dan seterusnya

Teorema 3.3 Pythagoras

Bilangan $\sqrt{2}$ adalah irasional

Bukti:

Andaikan $\sqrt{2}$ rasional, misal $\sqrt{2} = a/b$ dengan a dan b bilangan bulat positif dan gcd (a,b) = 1.

Jika kedua ruas dikuadratkan diperoleh $a^2 = 2b^2$ sehingga $b \mid a^2$.

Jika b > 1, berdasarkan teorema dasar aritmatika dijamin ada bilangan prima p sehingga $p \mid b$. Ini mengakibatkan $p \mid a^2$, dan berdasarkan teorema 3.1 disimpulkan $p \mid a$. Karena $p \mid a$ dan $p \mid b$, maka gcd (a,b) $\geq p > 1$ kontradiksi dengan pengandaian gcd (a, b) = 1.

Jika b = 1, maka $a^2 = 2$ hal ini tidak mungkin (tidak ada bilangan bulat yang dikalikan dengan dirinya sendiri sama dengan 2).

Dengan demikian pengandaian haruslah salah, dengan kata lain $\sqrt{2}$ bilangan irasional.

3. 2. SARINGAN ERATOSTHENES

Teorema 3.4 Euclid

Banyaknya bilangan prima adalah tak hingga.

Bukti:

Andaikan banyaknya bilangan prima itu terhingga dan misalkan

$p_1 = 2$, $p_2 = 3$, $p_3 = 5$ $p_4 = 7$, ... bilangan prima terakhir (terbesar) adalah p_n.

Tinjau bilangan bulat positif $P = (p_1 p_2 ... p_n) + 1$.

Karena P > 1, menurut teorema 3.2, maka P terbagi oleh beberapa bilangan prima p.

Tetapi $p_1, p_2, ..., p_n$ semuanya bilangan prima, sehingga p haruslah sama dengan salah satu dari $p_1, p_2, ..., p_n$.

Dari $p \mid P$ dan $p \mid p_1 p_2 ... p_n$ disimpulkan $p \mid P - (p_1 p_2 ... p_n)$ atau $p \mid 1$. Karena p bilangan positif haruslah p = 1. Ini bertentangan dengan p > 1. Jadi banyaknya bilangan prima adalah tak hingga.

Teorema 3.5

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

Bukti:

Untuk n = 1 benar, sebab $2 \leq 2^{2^{1-1}} = 2^{2^0} = 2^1 = 2$

Misalkan untuk n = k > 1 benar, artinya $p_k \leq 2^{2^{k-1}}$

Akan ditunjukkan bahwa untuk n = k + 1 juga benar.

Perhatikan

$p_{k+1} \le p_1 p_2 \ldots p_k + 1 \le 2.2^2 \ldots 2^{2^{k-1}} + 1 = 2^{(1+2+2^2+\ldots+2^{k-1})} + 1$

Ingat identitas $1 + 2 + 2^2 + \ldots + 2^{k-1} = 2^k - 1$

Dengan demikian kita peroleh $p_{k+1} \le 2^{2^k - 1} + 1$

Karena $1 \le 2^{2^k - 1}$ untuk setiap k, maka diperoleh

$p_{k+1} \le 2^{2^k - 1} + 2^{2^k - 1} = 2.2^{2^k - 1} = 2^{2^k} = 2^{2^{(k+1)-1}}$

Corollary

Untuk $n \ge 1$, paling sedikit terdapat n+1 bilangan prima yang kurang dari 2^{2^n}

Bukti:

Dari teorema 3.5 di atas kita mengetahui bahwa

p_1, p_2, ..., p_{n+1} kurang dari 2^{2^n}

Jika a > 1 dan a bilangan komposit, maka dapat ditulis a = bc dimana 1 < b < a dan 1 < c < a. Dengan mengasumsikan b ≤ c, diperoleh $b^2 \le bc = a$ atau $b \le \sqrt{a}$.

Karena b > 1, menurut teorema 3.2 b memiliki paling sedikit sebuah faktor prima p, dimana $p \le b \le \sqrt{a}$.

Selanjutnya karena p | b dan b | a maka p | a. Dari sini disimpulkan bahwa jika a bilangan komposit akan selalu memiliki sebuah faktor prima p yang memenuhi p peroleh≤ $\sqrt{a}$.

Tinjau a = 509, karena $22 < \sqrt{509} < 23$, kita akan coba bilangan prima yang lebih kecil 22, yaitu 2,3,5,7,11,13,17,19. Adakah yang membagi 509 ? Ternyata tidak ada, dengan demikian dapat disimpulkan 509 bilangan prima.

Contoh 3.1

Salah satu teknik untuk menyatakan suatu bilangan bulat dalam bentuk kanonik adalah sebagai berikut:

Misalkan a = 2093, karena $45 < \sqrt{2093} < 46$, kita cukup mencoba bilangan-bilangan prima 2,3,5,7,11,13,17,19,23,29,31,37,41,43.

Setelah dicoba ternyata 7 membagi 2093 dan 2093 = 7. 299.

Kemudian lakukan hal yang sama untuk bilangan 299.
Karena $17 < \sqrt{299} < 18$ ada tujuh bilangan prima yang lebih kecil dari 18 yaitu: 2,3,5,7,11,13,17. Setelah dicoba bilangan prima yang membagi 299 adalah 13 dan $299 = 13.23$. Karena 23 bilangan prima, maka $2093 = 7.13.23$.