NOMBOR PERDANA

OLEH

LEE HONG NAI

Projek diserahkan untuk memenuhi
sebahagaian keperluan bagi
Ijazah Sarjana Matematik Pengajaran

JUN 2008

PENGHARGAAN

Terlebih dahulu saya ingin mengucapkan jutaan terima kasih kepada penyelia projek saya iaitu Puan Ena Binti Jamal. Beliau telah mengorbankan banyak masa memberi tunjuk ajar, cadangan, sokongan dan bimbingan kepada saya sepanjang proses melengkapkan kerja projek ini.

Saya juga ingin mengucapkan terima kasih kepada semua pensyarah dan staff dari Pusat Pengajian Sains Matematik, USM yang telah banyak memberi bantuan dan sokongan.Di sini, saya juga ingin mengambil kesempatan mengucapkan terima kasih dan penghargaan yang setinggi-tingginya kepada Tuan Haji Said Bin Mohd Radzi, Pengetua Sekolah Menengah Kebangsaan Tunku Putera, Baling, Kedah, semua guru dan staf sokongan Sekolah Menengah Kebangsaan Tunku Putera yang telah memberi komitmen yang tinggi sepanjang pengajian saya.

Saya juga tidak lupa kepada keluarga tersayang saya yang selalu memberi sokongan kepada saya sepanjang tempoh pengajian saya.

ISI KANDUNGAN

		Muka Surat
PENGHARGAAN		ii
SENARAI JADUAL		vi
SENARAI RAJAH		vii
ABSTRAK		viii
ABSTRACT		ix
BAB 1 – PENGENALAN		
1.1	Nombor Perdana Dan Nombor Gubahan	1
1.2	Sejarah Perkembangan Nombor Perdana	3
BAB 2 - ELEMEN DALAM TEORI NOMBOR		
2.1	Prinsip Urutan Wajar (*Well Ordering Principle*)	7
2.2	Pembahagian Tepat	7
2.3	Kongruen	9
2.4	Pembahagian Tepat Oleh Integer Kecil	12
BAB 3 – PEMFAKTORAN DAN TEOREM-TEOREM NOMBOR PERDANA		
3.1	Nombor Perdana Dan Pemfaktoran	16
3.2	Pemfaktoran	17
3.3	Pemfaktoran Nombor Perdana	30

3.5 Rumus Nombor Perdana 36

3.6 Taburan Nombor Perdana 39

BAB 4 – JENIS NOMBOR PERDANA

4.1 Mersenne 44

4.2 Fermat 47

4.3 Kembar 49

4.4 Faktorial dan Primorial 50

4.5 Sophia Germain 52

4.6 Wieferich 53

4.7 Wilson 54

4.8 Wall-Sun-Sun 54

4.9 Wolstenholme 55

4.10 Nowman-Shanks-Williams (NSW) 55

4.11 Smarandache-Wellin 56

4.12 Wagstaff 56

BAB 5 – NOMBOR PERDANA TERBESAR

5.1 Sebelum Era Komputer 58

5.2 Era Komputer 59

6.1 PRIME ialah Nombor Perdana 62

6.2 Nombor Perdana Berturutan 62

6.3 Nombor Perdana Berpola 65

6.4 Nombor Perdana Daripada Faktorial 67

6.5 Nombor Perdana Bertuah 68

6.6 Nombor Perdana Cermin 68

6.7 Nombor Perdana Tiga Digit 69

6.8 Segiempat sama Sempurna 70

6.9 Bentuk Segitiga Bersudut Tepat 71

BAB 7 – KRIPTOGRAFIK 72

BAB 8 – KESIMPULAN DAN CADANGAN 83

BIBLIOGRAFI 85

SENARAI JADUAL

Muka Surat

Jadual 3.2.2.1 : Langkah 1 Algoritma Euclid Untuk Mencari (a, b) 22

Jadual 3.2.2.2 : Langkah 2 Algoritma Euclid Untuk Mencari (a, b) 22

Jadual 3.2.2.3 : Langkah 3 Algoritma Euclid Untuk Mencari (a, b) 23

Jadual 3.2.2.4 : Langkah 4 Algoritma Euclid Untuk Mencari (a, b) 23

Jadual 3.2.2.5 : Langkah 5 Algoritma Euclid Untuk Mencari (a, b) 24

Jadual 3.4.2.1 : Nombor Perdana Dalam Lingkungan 100. 36

Jadual 3.4.2.2 : Nombor Perdana Dalam Lingkungan 1000. 36

Jadual 3.5.1 : Nombor Perdana p Di mana $n < p < 2n$. 39

Jadual 3.6.1.1 : Nilai $\pi(x)$ 40

Jadual 3.6.2.1 : Penghampiran $\pi(x)$ Oleh $\frac{x}{\ln x}$ 42

Jadual 4.1.1 : Contoh Nombor Mersenne 45

Jadual 4.1.2 : 44 Nombor Perdana Mersenne 46

Jadual 4.3.1 : Sepuluh Nombor Perdana Kembar Terbesar 50

Jadual 4.4.1 : Sepuluh Nombor Perdana Faktorial Terbesar 51

Jadual 4.4.2 : Sepuluh Nombor Perdana Primorial Terbesar 52

Jadual 4.5.1 : Sepuluh Nombor Perdana Sophia Germain Terbesar 53

Jadual 5.1.1 : Rekod Nombor Perdana Terbesar Sebelum Era Komputer 59

Jadual 5.2.1 : Sepuluh Nombor Perdana Terbesar 61

Jadual 6.5.1 : Nombor Perdana Bertuah 68

Jadual 7.1 : Huruf A Hingga Z Yang Setara Dengan Angka 0 Hingga 26 73

SENARAI RAJAH

Muka Surat

Rajah 4.1.1 : Setem Bagi Nombor Perdana Mersenne ke-23 47

ABSTRAK

Teori Nomber ialah bidang Matematik yang menarik minat dan perhatian semua sejak beribu-ribu tahun dahulu. Ia digelar sebagai "Ratu bagi Matematik' oleh Gauss.

Di Malaysia para pelajar didedahkan dengan pelbagai jenis nombor. Para pelajar mula diperkenalkan dengan nombor perdana sejak di tingkatan satu lagi. Tetapi, apabila ditanyakan apa itu nombor perdana, ramai pelajar malahan guru hanya boleh memberi jawapan "*nombor yang hanya boleh dibahagi oleh 1 dan dirinya*". Mereka tidak dapat memberi penerangan lanjut mengenai soalan ini. Oleh sebab inilah, telah mendorong saya untuk menjadikan Nombor Perdana sebagai tajuk projek saya.

Objektif utama projek ini adalah supaya ia dapat memberi gambaran lengkap dan pengetahuan penuh mengenai nombor perdana. Projek ini membincangkan tentang sejarah perkembangan nombor perdana, teorem-teorem yang berkaitan dengan nombor perdana, cara mengenali nombor perdana, jenis-jenis nombor perdana, nombor perdana terbesar yang dijumpai sehingga hari ini dan aplikasi nombor perdana dalam kriptografik. Selain daripada itu, pelbagai paten dan pola yang boleh dibentuk dengan nombor perdana juga disenaraikan.

Pendek kata diharap para pembaca akan tertarik dan mendapat manfaat serta idea setelah membaca laporan projek ini.

PRIME NUMBERS

ABSTRACT

The Number Theory is an interesting field of Mathematics and it has attracted the fascination and attention of many since thousand of years ago. Gauss called it 'The Queen for Mathematics.'

In Malaysia, students are exposed with various numbers. Both the previous curriculum and the present Integrated Curriculum introduces the secondary students to the prime number in form one itself. However, when asked to explain what prime number is, almost all students and even teachers themselves could only say that 'prime number is any number that is divisible by one and by itself.' They could not give a more suitable explanation than this. In view of this, it has encouraged me to explore prime numbers as my project topic.

The main objectives of this project are to give a complete full picture and a holistic knowledge concerning prime numbers. This project will discuss the history of the development of the prime numbers, the theorems related with prime numbers, types of prime numbers, the biggest prime number found to date, prime numbers patterns and structures, and the application of prime numbers in cryptographic.

It is hoped this project will fascinate and benefit the readers as well as generate ideas as they read this project.

BAB 1

PENGENALAN

1.1 Nombor Perdana Dan Nombor Gubahan

Sebahagian besar daripada integer boleh difaktorkan kepada dua atau lebih faktor yang lebih kecil, contohnya

$$6 = 2 \cdot 3$$
$$9 = 3 \cdot 3$$
$$30 = 2 \cdot 3 \cdot 5 = 3 \cdot 10$$

Manakala ada sesetengah integer tidak boleh difaktorkan seperti 3, 7, 13, 37 dan sebagainya.

Secara umumnya, setiap integer c boleh diungkapkan sebagai hasil darab dua nombor a dan b iaitu

$$c = a \cdot b$$

di mana a dan b adalah faktor bagi c. Setiap integer juga boleh diungkapkan sebagai

$$c = 1 \cdot c = c \cdot 1$$

Di sini kita berminat dengan integer yang hanya boleh diungkapkan dalam bentuk $c = 1 \cdot c = c \cdot 1$ yang mana integer jenis ini disebut sebagai nombor perdana.

Takrif 1.1.1

Nombor perdana ialah integer positif yang lebih besar daripada 1 dan hanya boleh dibahagi tepat oleh dirinya dan 1.

Contoh 1.1.1

Integer 2, 3, 5, 7, 11, 13, 17, 19, 23 dan 29 adalah sepuluh nombor perdana yang pertama.

Takrif 1.1.2

Integer positif yang lebih besar daripada 1 dan bukan nombor perdana dipanggil sebagai nombor gubahan.

Contoh 1.1.2

Integer 4, 8, 10, 33 dan 111 adalah nombor gubahan kerana

$$4 = 2 \cdot 2$$
$$8 = 4 \cdot 2$$
$$10 = 5 \cdot 2$$
$$33 = 3 \cdot 11$$
$$111 = 3 \cdot 37$$

Takrifan nombor perdana tidak membenarkan 1 sebagai nombor perdana. Hal ini berlaku kerana 1 hanya terdapat satu faktor sahaja. Jadi, 1 bukan nombor perdana dan juga bukan nombor gubahan, manakala 2 adalah satu-satunya nombor perdana yang genap.

1.2 Sejarah Perkembangan Nombor Perdana

Dipercayai pada zaman purba Mesir lagi telah mula ada pengetahuan tentang nombor perdana iaitu perkembangan pecahan Mesir dalam *Rhind Papyrus*, tetapi terdapat perbezaan dengan nombor perdana hari ini. Catatan paling awal tentang nombor perdana adalah dari zaman Yunani. Kira-kira pada 300 sebelum masihi, sekolah Pythagoras di zaman Yunani telah mula membezakan nombor perdana dan nombor gubahan.

Pada awal Yunani, nombor 1 tidak termasuk dalam senarai nombor perdana. Pada masa itu, 1 juga tidak termasuk dalam senarai nombor kerana nombor 1 hanya dipanggil sebagai dasar bagi nombor (*principle of number*). Euclid dan Aristotle terima nombor 2 sebagai nombor perdana tetapi pada awalnya Pythagoras tidak, kerana beliau menggelarnya sebagai dasar bagi nombor genap (*principle of even*). Pendek kata, sebelum abad ke-19, ramai ahli matematik menyatakan bahawa 1 ialah nombor perdana. Dipercayai Henri Lebesgue ialah ahli matematik terakhir yang menyatakan 1 ialah nombor perdana.

Euclid memulakan perkembangan teori bagi nombor perdana apabila beliau membuktikan bahawa set nombor perdana adalah tak terhingga. Selepas Euclid, pada 230 sebelum masihi, Eratosthenes mencipta cara untuk menguji keperdanaan sesuatu nombor iaitu '*sieve*' yang membawa maksud penapisan atau saringan. Dalam masa lebih kurang 20 tahun selepas ini, beberapa keputusan penting telah diperkembangkan dalam menguji keperdanaan sesuatu nombor.

keperdanaan sesuatu nombor, n, iaitu dengan membahagikan n dengan nombor bulat kurang daripada $\sqrt{n}$. Selepas ini, beliau percaya bahawa nombor perdana dapat ditulis dalam bentuk $2^{2^n}+1$ (kemudianya digelar sebagai Nombor Fermat, F_n). Malangnya, beliau hanya dapat mengesahkan nombor perdana dalam bentuk $2^{2^n}+1$ sehingga n = 4. Pada tahun 1732, Leonhard Euler telah membuktikan bahawa F_5 iaitu $2^{32}+1$ bukan nombor perdana. Selepas ini, dipercayai bahawa tiada nombor perdana bagi F_n selain daripada n = 0, 1, 2, 3, dan 4.

Pada abad ke-18 dan ke-19, banyak masa telah digunakan untuk menguji keperdanaan sesuatu nombor dengan mencari faktor bagi nombor gubahan. Pada tahun 1772, Euler telah membina satu formula bagi set nombor perdana dalam $0 \le n \le 40$ iaitu n^2-n+41 , tetapi formula ini gagal bagi $n=41$. Pada tahun 1879 pula, E.B.Escott telah mencipta formula $n^2-79n+1601$ yang mana dapat memberi set nombor perdana bagi semua n = 0, 1, 2, ... , 79, tetapi ia juga gagal bagi n = 80. Banyak cubaan telah dibuat dan telah dibuktikan bahawa tiada fungsi polinomial yang hanya dapat membentuk set nombor perdana sahaja. Ahli Matematik Perancis, Marin Mersenne mengkaji nombor perdana dalam bentuk 2^p-1, di mana p ialah nombor perdana. Nombor bentuk ini dipanggil sebagai nombor Mersenne. Pada 1961 nombor perdana terbesar yang dapat dicari ialah $2^{3,217}-1$, iaitu satu nombor yang mempunyai 969 digit. Pada tahun 1965, nombor ini telah digantikan dengan $2^{11,213}-1$ yang mempunyai 3 376 digit.

mengenai nombor perdana iaitu apabila x menghampiri ∞, bilangan bagi nombor perdana sehingga x adalah menghampiri $\frac{x}{\ln x}$. Pada tahun 1896, Jacques Hadamand dan C.J. de La Vallée-Poussin telah membuktikan konjektor ini. Lanjutan daripada ini, teorem ini menyatakan bahawa jika $\pi(x)$ ialah nombor perdana kurang daripada integer x, maka $\log_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$, dan ianya digelar sebagai Teorem Nombor Perdana (*Prime Number Theorem*).

Cara membuktikan nombor perdana adalah tidak mudah jika nombor itu adalah besar nilainya. Ramai ahli Matematik telah mengorbankan sepanjang hayat untuk membuktikan keperdanaan bagi sesuatu nombor yang besar. Ia biasanya dihadkan kepada nombor dalam sesuatu bentuk sahaja seperti ujian Pépin untuk nombor Fermat (pada tahun 1877), teorem Proth (kira-kira 1878), ujian Lucas-Lehmer untuk nombor Mersenne (mula pada tahun 1856) dan sebagainya.

Sebelum tahun 1970, nombor perdana dipercayai tiada kegunaan lain selain daripada dalam matematik tulen. Anggapan ini telah berubah setelah konsep bagi kriptografik iaitu tulisan rahsia dengan nombor perdana sebagai asas dalam algoritma telah dicipta. Nombor perdana telah digunakan dalam tulisan rahsia supaya menjamin kesulitannya.

Bermula daripada tahun 1951, tugas mengesahkan nombor perdana terbesar telah diambilalih oleh komputer. Pada tahun 1996, George Woltman telah mencipta *The Great Internet Mersenne Prime Seach* (GIMPS) untuk mencari nombor perdana

mempunyai 9 808 358 digit iaitu $2^{32,582,657}-1$ yang telah diumumkan oleh GIMPS pada 4 September 2006. Usaha mencari nombor perdana terbesar masih diteruskan dan dipercayai ia tidak akan berakhir sebab nombor perdana adalah tak terhingga.

BAB 2

ELEMEN DALAM TEORI NOMBOR

2.1 Prinsip Urutan Wajar (*Well Ordering Principle*)

Apabila diberi satu set S, di mana $S \subset N$ (Set Nombor Asli), untuk mencari unsur terkecil dalam set S adalah senang. Ia dapat dilakukan dengan membanding setiap unsur dalam set S sebab set S adalah terhad. Bagaimana kalau set S adalah tak terhingga? Jadi, di sini diperkenalkan satu teorem mengenai hal ini, tidak kira set itu terhingga atau tak terhingga.

Teorem 2.1.1 (Prinsip Urutan Wajar)

Biar set S bukan set kosong dan $S \subset N$. Set S terdapat satu unsur terkecil dalamnya.

2.2 Pembahagian Tepat

Apabila sesuatu integer dibahagi oleh integer lain yang bukan sifar, hasil bahaginya mungkin bukan sesuatu integer. Sebagai contoh, 24/6 = 4 ialah satu integer, manakala 24/5 = 4.8 bukan integer. Hal ini telah menghasilkan takrifan di bawah.

Katakan a dan b ialah integer di mana $a \neq 0$, b dikatakan boleh dibahagi tepat oleh a jika terdapat satu integer c di mana $b = ac$.

Jika b boleh dibahagi tepat oleh a, a adalah faktor bagi b dan boleh ditulis sebagai $a|b$.

Jika b tidak boleh dibahagi tepat oleh a, kita tulis sebagai $a \nmid b$.

Contoh 2.2.1

$13|169$, $-2|20$, $14|0$, $13 \nmid 2$, $-7 \nmid 50$

Contoh 2.2.2

Hasil bahagi atau faktor bagi 6 ialah ± 1, ± 2, ± 3, dan ± 6.

Hasil bahagi atau faktor bagi 19 ialah ± 1 dan ± 19.

Berikut adalah ciri-ciri yang berkaitan dengan pembahagian tepat.

Teorem 2.2.1

Jika a, b dan c adalah integer di mana $a|b$ dan $b|c$, maka $a|c$

Contoh 2.2.3

Kita telah ketahui bahawa $3|18$ dan $18|72$, maka dengan Teorem 2.2.1, $3|72$.

Teorem 2.2.2

Diberi a, b, m, dan n adalah integer, jika $c|a$ dan $c|b$, maka $c|(ma + nb)$.

Diberi $3|21$ dan $3|33$. Dengan Teorem 2.2.2, $3|(5\cdot 21 - 3\cdot 33 = 6)$.

Teorem 2.2.3 Algoritma Pembahagian (*The Division Algotithm*)

Jika a dan b adalah integer dengan $b > 0$, maka terdapat satu integer q dan r di mana $a = bq + r$ dengan $0 \le r < b$.

Dalam algoritma pembahagian, q adalah hasil bahagi (*quotient*), r adalah baki (*remainder*), a adalah nombor yang dibahagi (*dividend*) dan b adalah pembahagi (*divisor*). b dikatakan boleh dibahagi tepat oleh a jika bakinya adalah sifar.

Contoh 2.2.5

Biar $a = 1028$ dan $b = 34$, maka $a = bq + r$ dengan $0 \le r < b$, di mana $q = [1028/34] = 30$ dan $r = 1028 - [1028/34]\cdot 34 = 1028 - 30\cdot 34 = 8$.

2.3 Kongruen

Konsep kongruen selalu muncul dalam kehidupan harian kita, sebagai contoh masa berfungsi dengan kongruen kepada 12 atau 24 bagi jam, 60 bagi minit dan saat dan kelander berfungsi dengan kongruen kepada 7 bagi hari atau 12 bagi bulan. Pada abad yang ke-19, ahli matematik yang bernama Karl Friedrich Gauss telah mula mengembangkan konsep kongruen.

Biar a dan b sebagai integer, a dikatakan kongruen kepada b modulo m jika dan hanya jika $m|(a-b)$, di mana m adalah integer positif. Ia juga boleh disimbolkan sebagai $a \equiv b(\mathrm{mod}\, m)$.

Contoh 2.3.1

$$5|(8-3) \quad \Leftrightarrow \quad 8 \equiv 3(\mathrm{mod}\, 5)$$
$$2|(-43-9) \quad \Leftrightarrow \quad -43 \equiv 9(\mathrm{mod}\, 2)$$

$$9 \nmid (13-5) = 8 \quad \Leftrightarrow \quad 13 \not\equiv 5 \ (\mathrm{mod}\ 9)$$

Bila a dibahagikan dengan m, andaikan hasil bahaginya ialah q dan bakinya ialah r, maka

$$a = mq + r, \qquad 0 \le r < m$$

Dengan andaian yang sama,

$$b = ml + s \qquad 0 \le s < m$$

Maka

$$a - b = m(q-l) + (r-s)$$

Jadi

$m|(a-b)$ jika dan hanya jika $m|(r-s)$.

bagaimanapun, $|r-s| < m$ supaya

$m|(a-b)$ jika dan hanya jika $r - s = 0$

lain mengenai konsep kongruen.

Teorem 2.3.1

Jika a dan b adalah integer, maka $a \equiv b(\text{mod}\, m)$ jika dan hanya jika terdapat satu integer k supaya $a = b + km$.

Contoh 2.3.2

Jika $19 \equiv -2(\text{mod}\, 7)$, maka $19 = -2 + 3 \cdot 7$

Teorem 2.3.2

Andaikan $a \equiv b\,(\text{mod}\, m)$ dan $c \equiv d(\text{mod}\, m)$, maka

i) $a + c \equiv (b + d)(\text{mod}\, m)$

ii) $a \cdot c \equiv (b \cdot d)(\text{mod}\, m)$

Teorem 2.3.3

i) $a \equiv b(\text{mod}\, m) \Rightarrow b \equiv a(\text{mod}\, m)$

ii) $a \equiv b(\text{mod}\, m)$ *and* $b \equiv c(\text{mod}\, m) \Rightarrow a \equiv c(\text{mod}\, m)$

iii) $a \equiv a(\text{mod}\, m)$

Bagi nombor 346 adalah jelas bahawa ia menunjukkan tiga ratus empat puluh enam, tetapi definasi ini agak keliru bagi abc. Untuk mengelakkan kekeliruan, kita menakrifkan $\overline{abc}$ sebagai nombor tiga digit, di mana

$$\overline{abc} = 10^2 a + 10^1 b + 10^0 c$$

Maka

$$\overline{a_{n-1}a_{n-2}a_{n-3}...a_1a_0} = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + 10^{n-3}a_{n-3} + ... + 10a_1 + a_0$$

Biarkan

$$x = \overline{a_{n-1}a_{n-2}a_{n-3}...a_1a_0} = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + 10^{n-3}a_{n-3} + ... + 10a_1 + a_0$$

Bahagian di bawah menunjukkan beberapa sifat bagi x untuk menyemak sama ada ianya boleh dibahagi tepat oleh beberapa integer kecil.

2.4.1 Pembahagian Tepat Oleh 2^k

Jika

$$x \equiv a_0 \pmod 2$$

maka

i) $2|x$ jika dan hanya jika $x \equiv 0 \pmod 2$

$2|x$ jika dan hanya jika $a_0 \equiv 0 \pmod 2$

$2|x$ jika dan hanya jika $2|a_0$.

Untuk menyemak sama ada sesuatu nombor x boleh dibahagi tepat oleh 2 atau tidak, kita hanya perlu menyemak digit a_0. Jika a_0 boleh dibahagi tepat dengan 2, maka x juga boleh dibahagi tepat dengan 2.

oleh 4, 8, 16 atau nombor asas 2 yang sebagainya.

ii) $4|x$ jika dan hanya jika $x \equiv 0 \pmod 4$

$4|x$ jika dan hanya jika $10a_1 + a_0 \equiv 0 \pmod 4$

$4|x$ jika dan hanya jika $4|\overline{a_1 a_0}$

iii) $8|x$ jika dan hanya jika $8|\overline{a_2 a_1 a_0}$

iv) Pendek kata, x boleh dibahagi tepat dengan 2^k jika dan hanya jika $2^k \mid \overline{a_{k-1} a_{k-2} \ldots a_1 a_0}$

2.4.2 Pembahagian Tepat Oleh 3 dan 9

i) $3|x$ jika dan hanya jika $3|\sum_{i=0}^{n-1} a_i$

ii) $9|x$ jika dan hanya jika $9|\sum_{i=0}^{n-1} a_i$

2.4.3 Pembahagian Tepat oleh 5^k

i) $5|x$ jika dan hanya jika $5|a_0$

ii) $25|x$ jika dan hanya jika $25|\overline{a_1 a_0}$

iii) $5^k|x$ jika dan hanya jika $5^k| \overline{a_{k-1} a_{k-2} \ldots a_1 a_0}$

i) $10|x$ jika dan hanya jika $10|a_0$

ii) $100|x$ jika dan hanya jika $100|\overline{a_1 a_0}$

iii) $10^k|x$ jika dan hanya jika $10^k| \overline{a_{k-1}a_{k-2}...a_1 a_0}$

2.4.5 Pembahagian Tepat oleh 7, 11 dan 13

i) $7|x$ jika dan hanya jika $7| (\overline{a_{n-1}a_{n-2}...a_3} - \overline{a_2 a_1 a_0})$

ii) $11|x$ jika dan hanya jika $11| (\overline{a_{n-1}a_{n-2}...a_3} - \overline{a_2 a_1 a_0})$ atau

$11|x$ jika dan hanya jika $11| (a_0 - a_1 + a_2 - a_3 + ... + (-1)a_{n-1})$ [setara dengan

$11| \sum_{i=0}^{n-1}(-1)^i a_i$]

iii) $13|x$ jika dan hanya jika $13| (\overline{a_{n-1}a_{n-2}...a_3} - \overline{a_2 a_1 a_0})$

Biar x = 843 145 796

Jadi,

$2 \mid x$ kerana $2 \mid 6$

$3 \nmid x$ kerana $3 \nmid (8 + 4 + 3 + 1 + 4 + 5 + 7 + 9 + 6 = 47)$

$4 \mid x$ kerana $4 \mid 96$

$5 \nmid x$ kerana $5 \nmid 6$

$6 \nmid x$ kerana $2 \mid x$ tetapi $3 \nmid x$

$7 \nmid x$ kerana $7 \nmid (843\ 145 - 796 = 842\ 349)$

$8 \nmid x$ kerana $8 \nmid 796$

$9 \nmid x$ kerana $9 \nmid (8 + 4 + 3 + 1 + 4 + 5 + 7 + 9 + 6 = 47)$

$10 \nmid x$ kerana $10 \nmid 6$

$11 \nmid x$ kerana $11 \nmid (6 - 9 + 7 - 5 + 4 - 1 + 3 - 4 + 8 = 9)$

$12 \nmid x$ kerana $4 \mid x$ tetapi $3 \nmid x$

$13 \nmid x$ kerana $13 \nmid (843\ 145 - 796 = 842\ 349)$

BAB 3

PEMFAKTORAN DAN TEOREM-TEOREM NOMBOR PERDANA

3.1 Nombor Perdana Dan Pemfaktoran

Nombor perdana adalah integer yang hanya mempunyai dua faktor sahaja iaitu dirinya dan 1 (Takrif 1.1.1). Di bawah ini telah disenaraikan beberapa teorem yang berkaiatan dengan nombor perdana dan pemfaktoran.

Takrif 3.1.1

Jika $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, di mana $p_1, p_2, \ldots, p_k$ adalah nombor perdana , maka $p_1, p_2, \ldots, p_k$ dipanggil sebagai faktor perdana bagi *n*.

Contoh 3.1.1

$30 = 2 \cdot 3 \cdot 5$, jadi 2, 3 dan 5 adalah faktor perdana bagi 30.

Setiap nombor yang lebih besar daripada 1 boleh dituliskan sebagai hasil darab bagi faktor-faktor perdananya. Cara menulis faktor perdana bagi setiap nombor adalah unik iaitu hanya terdapat satu cara sahaja untuk menulis hasil darab bagi faktor perdana. Walau bagaimanapun, susunan faktor perdana mungkin berbeza seperti :

$30 = 3 \cdot 2 \cdot 5$ atau $30 = 5 \cdot 2 \cdot 3$.

Setiap integer positif yang lebih besar daripada 1 terdapat faktor perdana.

Teorem 3.1.2

Set nombor perdana adalah tak terhingga.

Teorem 3.1.3

Jika n ialah nombor gubahan, maka terdapat faktor perdana yang kurang daripada $\sqrt{n}$.

Teorem ini boleh digunakan untuk mencari semua nombor perdana yang kurang atau sama dengan integer positif n. Proses ini dipanggil Kaedah Cuba Membahagi (*Trial Division*).

3.2 Pemfaktoran

3.2.1 Faktor Sepunya Terbesar (FSTB)

Jika a dan b adalah dua integer yang bukan sifar, di mana $d|a$ dan $d|b$, maka d adalah faktor sepunya bagi a dan b.

Contoh 3.2.1.1

$3|18$ dan $3|63$, jadi 3 adalah faktor sepunya bagi 18 dan 63.

$-3|18$ dan $-3|63$, jadi -3 juga adalah faktor sepunya bagi 18 dan 63.

faktor sepunya ini juga sentiasa mengandungi unsur +1 dan -1. Oleh kerana set faktor sepunya adalah terhingga, maka ia akan terdapat satu unsur yang terbesar nilainya. Kita berminat untuk mencari faktor sepunya terbesar di antara dua integer.

Takrif 3.2.1.1

Faktor sepunya terbesar bagi dua integer a dan b yang bukan sifar adalah faktor sepunya yang terbesar bagi kedua-dua a dan b dan ia disimbolkan sebagai (a, b).

Contoh 3.2.1.2

Faktor sepunya bagi 24 dan 84 adalah ± 1, ± 2, ± 3, ± 4, ± 6 dan ± 12.

Jadi $(24, 84) = 12$.

$a|b$ juga bermaksud $-a|b$, jadi faktor sepunya terbesar jika wujud ianya mesti integer positif. Jadi $(-a, b) = (a, -b)$, $(-a, -b) = (a, b)$.

Contoh 3.2.1.3

$(-24, 84) = (24, -84) = (-24, -84) = (24, 84) = 12$

Teorem 3.2.1.1

Jika a dan b adalah integer yang bukan sifar, maka (a, b) wujud.

Biar a, b, dan c sebagai integer dengan $(a, b) = d$, maka

i) $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

ii) $(a + cb, b) = (a, b)$

Teorem 3.2.1.3

Jika $0 < b \leq a$, maka $(a, b) = (a - b, b)$.

Teorem ini boleh digunakan untuk mencari FSTB bagi sebarang dua integer.

$$
\begin{aligned}
(1\,234, 4\,321) &= (1\,234,\ 4321 - 1\,234) \\
&= (1\,234, 3\,087) \\
&= (1\,234, 3\,087 - 1\,234) \\
&= (1\,234, 1\,853) \\
&= (1\,234, 1\,853 - 1\,234) \\
&= (1\,234, 619) \\
&= (1\,234 - 619, 619) \\
&= (615, 619) \\
&= (615, 619\text{-}615) \\
&= (615, 4) \\
&= (615 - 4, 4) \\
&= (611, 4) \\
&= (611\text{-}4, 4) \\
&= (507, 4) \\
&= (507 - 4, 4) \\
&= (503, 4) \\
&\ \ \vdots \\
&= (3, 4) = 1
\end{aligned}
$$

Teorem 3.2.1.4

Jika a dan b adalah dua integer yang bukan sifar, maka (a, b) wujud. Di samping itu, juga wujud dua integer α dan β supaya $(a,b) = \alpha a + \beta b$.

Algoritma Euclid ialah satu cara yang mudah untuk mencari FSTB bagi dua nombor terutamanya nombor yang besar. Algoritma Euclid ialah menggantikan masalah asal dengan cara yang lebih mudah dengan jawapan yang sama.

Biar integer a dan b di mana $a > b$. Untuk mencari (a, b), ikuti langkah di bawah :

$$
\begin{aligned}
a &= bq_1 + r_1 && (1)\\
b &= r_1 q_2 + r_2 && (2)\\
r_1 &= r_2 q_3 + r_3 && (3)\\
r_2 &= r_3 q_4 + r_4 && (4)\\
&\vdots\\
r_{n-1} &= r_n q_{n+1} + r_{n+1} && (n+1)\\
r_n &= r_{n+1} q_{n+2} + r_{n+2} && (n+2)\\
r_{n+1} &= r_{n+2} q_{n+3} && (n+3)
\end{aligned}
$$

Oleh kerana r_k adalah integer positif dan r_k akan jadi semakin kurang apabila k meningkat, kita akan sampai satu tahap di mana $r_k = 0$. Seperti algoritma yang ditunjukkan di atas, kita menganggap $r_{n+3} = 0$ dan kita dapat $r_{n+2} = (a,b)$.

Di sini, kita perlu mengungkapkan (a, b) dalam bentuk $\alpha a + \beta b$. Biarkan Q sebagai hasil bahagi dan R sebagai baki. Jadual 3.2.2.1 dibina supaya kita boleh dapat $R = ua + vb$ pada setiap baris. Kita mengikuti algoritma di bawah untuk mencari (a, b).

Jadual 3.2.2.1 : Langkah 1 Algoritma Euclid Untuk Mencari (a, b).

Q	*R*	*u*	*v*
	a	1	0
	b	0	1

Ini bermaksud $a = 1 \cdot a + 0 \cdot b$ pada baris pertama dan $b = 0 \cdot a + 1 \cdot b$ pada baris yang kedua.

Dengan menganggapkan $a > b$, apabila b dibahagikan dengan a, hasil bahaginya ialah q_1 dan bakinya ialah r_1 iaitu

$$a = bq_1 + r_1 \quad \Rightarrow \quad r_1 = a + (-q_1)b$$

Kita mengisikannya langkah ke-2 pada baris ketiga seperti yang ditunjukkan pada Jadual 3.2.2.2.

Jadual 3.2.2.2 : Langkah 2 Algoritma Euclid Untuk Mencari (a, b).

Q	*R*	*u*	*v*
	a	1	0
	b	0	1
q_1	r_1	1	$-q_1$

Baris ketiga menunjukkan $r_1 = 1 \cdot a + (-q_1)b$. Apabila b dibahagikan dengan r_1, hasil bahaginya ialah q_2 dan bakinya ialah r_2, iaitu

$$\Rightarrow \quad r_2 = b - (a - q_1 b)q_2$$

$$\Rightarrow \quad r_2 = (-q_2)a + (1 + q_1 q_2)b$$

Kita mengisikannya langkah ke-3 dalam Jadual 3.2.2.3.

Jadual 3.2.2.3 : Langkah 3 Algoritma Euclid Untuk Mencari (a, b)

Q	**R**	**u**	**v**
	a	1	0
	b	0	1
q_1	r_1	1	$-q_1$
q_2	r_2	$-q_2$	$1 + q_1 q_2$

Seperti yang ditunjukkan di atas, $r_2 = -q_2 a + (1 + q_1 q_2)b$. Dengan cara yang sama, apabila kita sampai baris ke-k dan baris ke-(k+1), kita akan dapat seperti yang ditunjukkan pada Jadual 3.2.2.4.

Jadual 3.2.2.4 : Langkah 4 Algoritma Euclid Untuk Mencari (a, b).

	Q	***R***	***u***	***v***
		a	1	0
		b	0	1
	q_1	r_1	1	$-q_1$
	q_2	r_2	$-q_2$	$1 + q_1 q_2$
		.		
		.		
		.		
baris ke-k	q_{k-2}	r_{k-2}	u_k	v_k
baris ke-(k+1)	q_{k-1}	r_{k-1}	u_{k+1}	v_{k+1}

$$r_{k-2} = u_k a + v_k b$$

$$r_{k-1} = u_{k+1} a + v_{k+1} b$$

Apabila r_{k-1} dibahagikan dengan r_{k-2}, hasil bahaginya ialah q_k dan bakinya ialah r_k,

$$r_{k-2} = r_{k-1} q_k + r_k \quad \Rightarrow \quad r_k = r_{k-2} - q_k r_{k-1}$$

iaitu

$$\Rightarrow \quad r_k = (u_k a + v_k b) - q_k (u_{k+1} a + v_{k+1} b)$$

$$\Rightarrow \quad r_k = (u_k - q_k u_{k+1}) a + (v_k - q_k v_{k+1}) b$$

Maka baris yang ke-(k+2) adalah seperti yang ditunjukkan dalam Jadual 3.2.2.5.

Jadual 3.2.2.5 : Langkah 5 Algoritma Euclid Untuk Mencari (a, b).

	Q	***R***	***u***	***v***
		a	1	0
		b	0	1
	q_1	r_1	1	$-q_1$
	q_2	r_2	$-q_2$	$1 + q_1 q_2$
		.		
		.		
		.		
baris ke-k	q_{k-2}	r_{k-2}	u_k	v_k
baris ke-(k+1)	q_{k-1}	r_{k-1}	u_{k+1}	v_{k+1}
baris ke-(k+2)	q_k	r_k	$u_k - u_{k+1} q_k$	$v_k - v_{k+1} q_k$

Algoritma di atas digunakan untuk mencari (a, b).