2 BILANGAN PRIMA

Bilangan prima telah dikenal sejak sekolah dasar, yaitu bilangan yang tidak mempunyai faktor selain dari 1 dan dirinya sendiri. Bilangan prima memegang peranan penting karena pada dasarnya konsep apapun yang dibahas dalam teori bilangan selalu dikaitkan dengan bilangan prima. Sebagai ilustrasi, jika ditanyakan banyak faktor positif dari 24 maka biasanya dilakukan dengan mendaftar semua faktor tersebut yaitu $1, 2, 3, 4, 6, 8, 12, 24$ jadi ada 8 buah. Untuk bilangan 60 mempunyai sebanyak 12 faktor positif. Cara mendaftarkan satu per satu semua faktor seperti ini tidaklah efektif khususnya untuk bilangan yang besar. Coba perhatikan $24 = 2^3 \cdot 3$ dan $60 = 2^2 \cdot 3 \cdot 5$. Dengan menambahkan 1 pada setiap pangkat prima, kemudian mengalikan mereka maka diperoleh banyaknya faktor prima. Untuk bilangan 24 terdapat $(3 + 1) \times (1 + 1) = 8$ faktor, dan untuk 60 terdapat $(2 + 1) \times (1 + 1) \times (1 + 1) = 12$ faktor.

Bagaimana juga ketika diminta untuk menentukan suatu bilangan prima atau bukan, bagaimana memutuskan suatu bilangan bulat besar dapat dibagi oleh bilangan bulat lain, bagaimana distribusi bilangan prima dalam $\mathbb{Z}$; semuanya akan dibahas pada bab ini.

2.1 Teorema Fundamental Aritmatika

Definisi 2.1. Suatu bilangan bulat $p > 1$ dikatakan **prima** jika faktor positifnya hanyalah 1 dan p (dirinya sendiri). Bilangan bulat lebih dari 1 yang bukan prima disebut **komposit.**

Diantara 10 bilangan bulat pertama, $2, 3, 5, 7$ adalah prima dan $4, 6, 8, 10$ adalah komposit. Berdasarkan definisi ini hanya ada satu bilangan prima yang genap yaitu. Bilangan 1 bukan prima dan bukan komposit. Suatu bilangan p adalah komposit jika ada bilangan bulat a dan b sehingga $p = ab$. Tentunya dipenuhi $0 < a, b < p$.

Untuk memulai pokok bahasan ini, diperhatikan fakta sederhana bahwa bilangan prima 3 dapat membagi 36. Kita juga mempunyai faktorisasi berikut

$$36 = 6 \times 6 = 9 \times 4 = 12 \times 3 = 18 \times 2.$$

Ternyata bilangan 3 dapat membagi minimal salah satu faktor di setiap perkalian tersebut. Sekarang diperhatikan pula bilangan komposit 4, yaitu $4|(2 \times 6)$ tetapi $4 \nmid 2$ dan $4 \nmid 6$.

Teorema 2.1. *Jika p prima dan $p|ab$ maka $p|a$ atau $p|b$.*

Bukti. Bila ternyata $p|a$ maka teorema terbukti, selesai. Bila $p \nmid a$ maka pastilah $\gcd(a,b) = 1$ sebab faktor p hanyalah 1 atau p. Berdasarkan Teorema **??**(2) disimpulkan $p|b$. ∎

Teorema ini menyatakan bahwa jika suatu bilangan prima p membagi perkalian dua bilangan bulat maka p pasti membagi salah satu diantara keduanya. Fakta ini dapat diperluas untuk bentuk perkalian beberapa bilangan bulat.

Akibat 2.1. *Bila p prima dan $p|a_1a_2\cdots a_n$ maka $p|a_k$ untuk suatu $k \in \{1, \cdots, n\}$.*

Bukti. Dibuktikan dengan menggunakan prinsip induksi matematika. Untuk $n = 1$, pernyataan berlaku secara otomatis. Untuk $n = 2$ pernyataan benar berdasarkan Teorema 2.1. Andaikan berlaku untuk $n = i$, yaitu $p|a_1a_2\cdots a_i \to p|a_k$ untuk suatu $k \in \{1, \cdots, i\}$. Untuk $n = i+1$, diketahui $p|(a_1a_2\cdots a_i)(a_{i+1})$. Berdasarkan Teorema 2.1 maka $p|a_1a_2\cdots a_i$ atau $p|a_{i+1}$, yakni $p|a_k$ untuk suatu $k \in \{1, \cdots, i+1\}$. ∎

Akibat 2.2. *Bila $p, q_1, \cdots, q_n$ semuanya prima dan $p|q_1q_2\cdots q_n$ maka $p = q_k$ untuk suatu $k \in \{1, \cdots, n\}$.*

Bukti. Berdasarkan akibat 2.1, $p|q_k$ untuk suatu $k \in \{1, \cdots, n\}$. Karena q_k prima maka tidak ada faktor lain selain 1 dan dirinya sendiri q_k. Jadi haruslah $p = q_k$. ∎

Pada awal bab ini telah diilustrasikan bahwa suatu bilangan bulat dapat disajikan dalam bentuk perkalian bilangan-bilangan prima. Formalisasi keadaan ini disajikan dalam bentuk Teorema Fundamental Aritmatika (TFA) yang merupakan batu pijakan dalam teori bilangan.

Teorema 2.2. *Setiap bilangan bulat positif $n > 1$ selalu dapat disajikan dalam bentuk perkalian bilangan-bilangan prima. Representasi ini tunggal terhadap urutan faktor-faktornya, yaitu*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \tag{2.1}$$

dimana $p_1, \cdots, p_k$ prima dan $e_1, \cdots, e_k$ eksponen bulat positif.

Bukti. Dibuktikan dengan menggunakan prinsip induksi kuat. Untuk $n = 2$ pernyataan benar, yaitu dengan mengambil $p_1 = 2$ dan $e_1 = 1$. Asumsikan $n > 2$ dan ekspresi (2.1) dipenuhi oleh setiap bilangan diantara 1 dan n, yaitu $m = p_1^{e_1} p_2^{e_2} \cdots p_{k_m}^{e_{k_m}}$ untuk setiap $m = 3, 4, \cdots, n-1$. Sekarang untuk bilangan n. Bila n prima maka tidak perlu dibuktikan lagi, karena ekspresi (2.1) terpenuhi secara otomatis. Jadi diasumsikan n komposit, yaitu terdapat bilangan bulat a dan b sehingga $n = ab$ dimana $0 < a, b < n$. Karena kedua a dan b kurang dari n maka berdasarkan hipotesis, mereka dapat disajikan sebagai perkalian bilangan-bilangan prima, katakan $a = q_1^{e_1} q_2^{e_2} \cdots q_{k_a}^{e_{k_a}}$ dan $b = r_1^{e_1} r_2^{e_2} \cdots r_{k_r}^{e_{k_r}}$ dimana para q_i dan r_k prima. Dengan membuat urutan baru dapat disajikan $n = ab = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Selanjutnya ditunjukkan ketunggalan representasi (2.1). Andai kita mempunyai dua bentuk representasi berikut

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t} \quad (\#).$$

Berlaku $p_1 | n$. Berdasarkan Akibat (2.1), $p_1 | q_j$ untuk suatu $j \in \{1, \cdots, t\}$. Dengan cara menyusun kembali maka kita dapat meletakan q_j diawal, katakan $q_j = q_1$. Karena $p_1$dan q_1 keduanya prima dan $p_1 | q_1$maka haruslah $p_1 = q_1$. Substitusi ke dalam persamaan $(\#)$ diperoleh

$$p_1^{e_1 - 1} p_2^{e_2} \cdots p_k^{e_k} = q_1^{f_1 - 1} q_2^{f_2} \cdots q_t^{f_t}.$$

Bila proses ini diteruskan dengan memasangkan faktor prima yang sama pada kedua ruas, kemudian melakukan kanselasi maka akan terjadi penghilangan faktor prima pada salah satu ruas. Bila ada salah satu ruas yang tidak habis faktor primanya maka akan terdapat bilangan 1 pada ruas lainnya sehingga 1 merupakan perkalian dari paling tidak dua bilangan prima p_i atau q_j. Hal ini tidaklah mungkin karena p_i dan q_j keduanya lebih dari 1. Jadi faktor-faktor prima pada kedua ruas saling menghabiskan. Untuk itu, setelah penyusunan ulang haruslah $k = t$, $p_i = q_i$ dan $e_i = f_i$. Terbukti representasi (2.1) tunggal. ∎

Salah satu manfaat faktorisasi prima kita dapat menghitung banyaknya faktor prima suatu bilangan bulat seperti diilustrasi pada awal bab ini.

Contoh 2.1. Tentukan faktorisasi prima dari 24 dan 60. Gunakan hasil anda untuk menghitung banyaknya faktor positif yang ada. Temukan faktor-faktor prima tersebut.

Penyelesaian. Dengan mudah kita dapat menemukan faktorisasi untuk 24, yaitu $24 = 2^3 \cdot 3$. Untuk menemukan semua faktor positifnya, diperhatikan tabulasi silang seperti diberikan pada Tabel 2.1 (kiri). Semua faktor yang dimaksud adalah $\{1, 2, 3, 4, 6, 8, 12, 24\}$ yaitu ada 8 faktor. Kalau diperhatikan dengan seksama, besarnya pangkat pada faktorisasi prima menentukan banyak baris atau kolom pada tabulasi silang. Dalam hal ini pangkat 3 pada faktor 2^3 menghasilkan 4 kolom karena ditambahkan bilangan 1, sedangkan pangkat 1 pada $3^1 = 3$ menghasilkan 3 baris karena ditambahkan bilangan 1. Jadi banyak faktornya adalah $(3+1)\times(1+1) = 8$. Argumen yang sama diterapkan pada bilangan 60 yang mempunyai faktorisasi prima $2^2 \cdot 3 \cdot 5$. Bila diperhatikan Tabel 2.1 (kanan), kombinasi faktor 2^2 dan 3 menghasilkan $(2+1)\times(1+1) = 6$ buah faktor, yaitu $\{1, 2, 3, 4, 6, 12\}$. Kontribusi faktor 5 berikutnya memberikan faktor secara total adalah sebanyak $(2 + 1) \times (1 + 1) \times (1 + 1) = 12$ faktor, yaitu $\{1, 2, 3, 4, 6, 12, 5, 10, 15, 20, 30, 60\}$. Tabulasi silang seperti ini dapat membantu untuk menemukan semua faktor positifnya.

$\times$	1	2	2^2	2^3
1	1	2	4	8
3	3	6	12	24

$\times$	1	2	2^2			
1	1	2	4			
3	3	6	12			
$\times$	1	2	3	4	6	12
1	1	2	3	4	6	12
5	5	10	15	20	30	60

Table 2.1: Tabulasi silang faktor prima berpangkat

Berdasarkan pembahasan pada contoh soal ini diperoleh hasil sebagai berikut.

Teorema 2.3. *Bila $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ dan $\Pi(n)$ adalah banyak faktor positif dari n maka*

$$\Pi(n) = (e_1 + 1) \times (e_2 + 1) \times \cdots \times (e_n + 1). \quad (2.2)$$

Contoh 2.2. Tentukan semua faktor prima dari 50!, dan hitung banyak semua faktor positifnya.

Penyelesaian. Diperhatikan $50! := (50)(49)(48)\cdots(3)(2)(1)$. Jadi faktor-faktor primanya tidak lain adalah semua bilangan prima yang kurang dari 50, yaitu 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 (ada 15 buah). Untuk menghitung semua faktor positifnya, terlebih dahulu sajikan bilangan 50! dalam bentuk faktorisasi prima. Wow bilangannya besar sekali, bagaimana caranya? Salah satu caranya adalah dengan membentuk faktorisasi prima untuk masing-masing faktor kompositnya, yaitu:

$50 = 2 \cdot 5^2$	$42 = 2 \cdot 3 \cdot 7$	$34 = 2 \cdot 17$	$26 = 2 \cdot 13$	$18 = 2 \cdot 3^2$	$9 = 2^5 \cdot 5$
$49 = 7^2$	$40 = 2^3 \cdot 5$	$33 = 3 \cdot 11$	$25 = 5^2$	$16 = 2^4$	$8 = 2^3$
$48 = 2^4 \cdot 3$	$39 = 3 \cdot 13$	$32 = 2^5$	$24 = 2^3 \cdot 3$	$15 = 3 \cdot 5$	$6 = 2 \cdot 3$
$46 = 2 \cdot 23$	$38 = 2 \cdot 19$	$30 = 2 \cdot 3 \cdot 5$	$22 = 2 \cdot 11$	$14 = 2 \cdot 7$	$4 = 2^2$
$45 = 3^2 \cdot 5$	$36 = 2^2 \cdot 3^2$	$28 = 2^2 \cdot 7$	$21 = 3 \cdot 7$	$12 = 2^2 \cdot 3$	
$44 = 2^2 \cdot 11$	$35 = 5 \cdot 7$	$27 = 3^3$	$20 = 2^2 \cdot 5$	$10 = 2 \cdot 5$	

Jadi $50! = 2^{43}3^{20}5^{13}7^{8}11^{4}13^{3}17^{2}19^{2}23^{2}29^{1}31^{1}37^{1}41^{1}43^{1}47^{1}$ sehingga terdapat sebanyak $(44)(21)(14)(9)(5)(4)(3)(3)(3)(2)(2)(2)(2)(2)(2) = 4023613440$ buah, suatu jumlah yang sangat besar. ■

Contoh 2.3. Bila p prima dan $p|a^n$, buktikan $p^n|a^n$.

Bukti. Karena $p|\underbrace{aa\cdots a}_{n\,faktor} = a^n$ maka menurut Akibat 2.1 diperoleh $p|a$. Akibatnya, $p^n|a^n$. ■

Misalkan untuk dua bilangan bulat a dan b mempunyai representasi berikut

$$a = \prod_{i=1}^{r} p_i^{\alpha_i},\ b = \prod_{i=1}^{r} p_i^{\beta_i}$$

dimana lambang Π menyatakan perkalian suku-suku, layaknya notasi $\sum$ untuk penjumlahan. Kita selalu dapat menyatakan p_i sebagai faktor persekutuan dari a dan b dengan membolehkan α_i dan β_i bernilai nol. Dengan menggunakan representasi ini, maka diperoleh hasil berikut

$$\begin{aligned} ab &= \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i} \\ \frac{a}{b} &= \prod_{i=1}^{r} p_i^{\alpha_i-\beta_i} \text{ asalkan } b|a \\ \gcd(a,b) &= \prod_{i=1}^{r} p_i^{\min\{\alpha_i,\beta_i\}} \\ \operatorname{lcm}(a,b) &= \prod_{i=1}^{r} p_i^{\max\{\alpha_i,\beta_i\}} \end{aligned}$$

Contoh 2.4. Tentukan FPB dan KPK dari 132 dan 400.

Penyelesaian. Pertama ditentukan faktorisasi prima kedua bilangan ini, yaitu

$$\begin{aligned} 132 &= 2^2 \cdot 3 \cdot 11 \\ 400 &= 2^4 \cdot 5^2. \end{aligned}$$

Dengan menuliskan semua faktor prima yang ada, diperoleh $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 11$ dan $\alpha_1 = 2, \beta_1 = 4, \alpha_2 = 1, \beta_2 = 0, \alpha_3 = 0, \beta_3 = 2, \alpha_4 = 1, \beta^4 = 0$. Dengan demikian diperoleh

$$\begin{aligned} \gcd(132, 400) &= 2^2 \cdot 3^0 \cdot 5^0 \cdot 11^0 = 4 \\ \operatorname{lcm}(132, 400) &= 2^4 \cdot 3^1 \cdot 5^2 \cdot 11^1 = 13200. \end{aligned}$$

2.2 Saringan Eratosthenes

Bila diberikan sebuah bilangan bulat, bagaimana kita dapat memutuskan apakah ia prima atau komposit. Kalau ia komposit, bagaimana menentukan faktor-faktornya.

Teorema 2.4. *Sebuah bilangan bulat $n > 1$ adalah komposit bila hanya bila ia dapat dibagi oleh suatu faktor prima $p \leq \sqrt{n}$.*

Bukti. ($\leftarrow$) Bila n dapat dibagi oleh bilangan prima p tersebut maka jelas n komposit. ($\rightarrow$) Sebaliknya diketahui n komposit, maka dapat ditulis $n = ab$ dengan $0 < a, b < n$. Ini berakibat $a \leq \sqrt{n}$ atau $b \leq \sqrt{n}$, sebab bila tidak akan menghasilkan

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Gambar 2.1: Hasil saringan Eratosthenes

$ab > n$. Faktor a atau b ini pasti dapat dibagi oleh bilangan prima $p \leq \sqrt{n}$, yang juga kemudian membagi n. ■

Teorema ini mengatakan bahwa jika suatu bilangan bulat n tidak terbagi oleh setiap bilangan prima p dengan $p \leq \sqrt{n}$ maka dipastikan n adalah prima. Hasil inilah yang digunakan oleh seorang matematikawan Yunani Eratosthenes (276-194 SM) menemukan teknik untuk memilih bilangan prima dalam rentang tertentu. Metoda ini disebut **saringan Eratosthenes** (*sieve of Eratosthenes*). Metoda ini akan jelas dalam contoh menentukan semua bilangan prima yang kurang dari 100.

1. Daftarkan semua bilangan tersebut, yaitu $2, 3, \cdots, 100$. Dapat dibentuk dalam bentuk persegi panjang untuk menghemat tempat.

2. Biarkan bilangan 2 sebagai bilangan prima pertama, silang semua bilangan kelipatan 2, yaitu $4, 6, 8, \cdots$

3. Setelah 2, bilangan pertama tidak tercoret adalah 3. Pertahankan bilangan 3 sebagai prima kedua, silang semua kelipatan 3, yaitu $6, 9, 12, \cdots$.

4. Bilangan pertama setelah 3 yang belum tercoret mestinya 5. Pertahankan bilangan 5 ini, coret semua kelipatan 5, yaitu $10, 15, 20, \cdots$

5. Cara yang sama dilakukan pada bilangan 7.

Diperhatikan 7 adalah bilangan prima terakhir dengan $7 \leq \sqrt{100}$, sebab prima berikutnya adalah 11. Jadi setelah langkah ke 5, bilangan dalam daftar yang tidak tercoret adalah bilangan prima. Bilangan prima yang dimaksud adalah 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,41,43,47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, kesemuanya prima kurang dari 100. Hasil algoritma ini diberikan pada Gambar 2.1.

Contoh 2.5. Nyatakan $a = 2093$ dalam bentuk perkalian bilangan prima berpangkat.

Penyelesaian. Diperhatikan bahwa $\sqrt{2093} < 46$. Jadi cukup diperiksa bilangan prima yang kurang dari 46: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 yang merupakan faktor. Ternyata 2093 hanya memiliki tiga faktor prima, yaitu 17, 13 dan 23, tepatnya

$$2093 = 13 \cdot 17 \cdot 23. \quad \blacksquare$$

2.3 Distribusi Bilangan Prima

Diperhatikan terdapat 4 bilangan prima diantara 1 dan 10, ada 21 bilangan prima diantara 10 dan 100, ada 21 bilangan prima diantara 100 dan 200, ada 16 bilangan prima diantara 200 dan 300...... Berdasarkan data empiris ini, distribusi bilangan prima semakin lama semakin jarang. Mungkinkah suatu saat bilangan prima tidak muncul lagi diantara kumpulan bilangan bulat yang sangat besar. Teorema berikut memberian jawabannya. Teorema ini dikenal dengan **Teorema Euclides.**

Teorema 2.5. *Terdapat takberhingga banyak bilangan prima.*

Bukti. Dibuktikan dengan kontradiksi. Andai hanya terdapat berhingga banyak bilangan prima, katakan secara berurutan $p_1 = 2, p_2 = 3, \cdots, p_n$. Ambil bilangan bulat N yang didefinisikan sebagai

$$N = p_1 p_2 \cdots p_n + 1.$$

Karena $N > 1$ maka berdasarkan TFA, P mesti dapat dibagi oleh suatu bilangan prima p. Tetapi kita telah mengandaikan bahwa hanya $p_1, p_2, \cdots, p_n$ bilangan prima yang ada. Jadi haruslah $p = p_k$ untuk suatu $k \in \{1, \cdots, n\}$. Kita mempunyai dua fakta, yaitu $p|N$ dan $p|p_1p_2 \cdots p_n$. Akibatnya $p|(N - p_1p_2 \cdots p_n)$ atau $p|1$. Hal ini menimbulkan kontradiksi karena $p > 1$. Jadi tidaklah benar bahwa banyaknya bilangan prima berhingga. $\blacksquare$

Pembahasan mengenai bilangan prima banyak menyimpan misteri yang belum terkuak. Sampai saat ini belum ada formula eksplisit atau cara efektif untuk mengidentifikasi bilangan prima. Diperhatikan contoh berikut.

Contoh 2.6. Misalkan $p_1, p_2, \cdots, p_n$ adalah n buah bilangan prima pertama, dan didefinisikan $p_n^* = p_1 p_2 \cdots p_n + 1$. Selidikilah apakah untuk setiap $n \in \mathbb{N}$, p_n^* prima. Berikan komentar.

Penyelesaian. Kita selidiki untuk beberapa

$$\begin{aligned} p_1^* &= 2+1=3 \\ p_2^* &= 2\cdot 3+1=7 \\ p_3^* &= 2\cdot 3\cdot 5+1=31 \\ p_4^* &= 2\cdot 3\cdot 5\cdot 7+1=211 \\ p_5^* &= 2\cdot 3\cdot 5\cdot 7\cdot 11+1=2311, \end{aligned}$$

semuanya adalah prima. Namun perhatikan kasus berikut ini

$$\begin{aligned} p_6^* &= 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13+1=59\cdot 509 \\ p_7^* &= 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17+1=19\cdot 97\cdot 277, \end{aligned}$$

ternyata tidak prima. Ternyata tidak semua n, p_n^* prima. Permasalahan selanjutnya adalah tidak dapat diketahui dengan pasti apakah bilangan prima dengan pola seperti ini berhingga atau takberhingga. Sampai saat ini baru ditemukan 2, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801, dan 24029 bilangan prima yang mengikuti pola ini. Terakhir, sebuah bilangan prima bentuk ini ditemukan pada tahun 1995 terdiri dari 10395 digit. Selain itu, semua p_n^* dengan $n < 35000$ adalah komposit. ■

Teorema 2.6. *Terdapat takberhingga banyak bilangan prima yang berbentuk* $4q+3$.

Bukti. Bukti dengan kontradiksi. Andai hanya terdapat berhingga bilangan prima bentuk ini, katakan $p_1, p_2, \cdots, p_k$. Ambil $m = 4p_1p_2\cdots p_k - 1$ sehingga m berbentuk $4q+3$ yaitu dengan mengambil $q = p_1p_2\cdots p_k + 1$. Karena m ganjil maka setiap bilangan prima p yang membagi m juga ganjil, atau secara ekuivalen berbentuk $p = 4q+1$ atau $p = 4q+3$. Ingat adanya faktor prima ini dijamin oleh TFA. Bila p berbentuk $4q+1$ maka m juga mempunyai bentuk ini, padahal m berbentuk $4q+3$. Jadi haruslah m terbagi oleh suatu bilangan prima p yang berbentuk $4q+3$. Karena diasumsikan hanya ada $p_1, p_2, \cdots, p_k$ bilangan prima bentuk ini maka haruslah $p = p_i$ untuk suatu $i \in \{1, \cdots, k\}$. Jadi $p|p_1p_2\cdots p_k$, dan juga $p|m$. Diperoleh $p|4p_1p_2\cdots p_k - m$, atau $p|1$ suatu kontradiksi. ■

Contoh 2.7. Temukan 5 bilangan prima yang mempunyai pola $4q+1$.

Penyelesaian. Untuk $q = 1$ diperoleh $4(1)+1 = 5$, untuk $q = 3$ diperoleh $4(2)+1 = 13$, untuk $q = 4$ diperoleh $4(4) + 1 = 17$, untuk $q = 7$ diperoleh $4(7) + 1 = 29$, untuk $q = 9$ diperoleh $4(9) + 1 = 37$. ■

Sebaliknya tidak semua bilangan prima berbentuk $4q + 1$, misalnya 7, 11, 19 dan lain-lain. Jadi walaupun takberhingga banyak bilangan prima dalam bentuk ini, namun masih terdapat takberhingga banyak pula bilangan prima yang tidak berbentuk seperti ini. Tidak semua bilangan prima dapat dikenali bentuk umumnya. Sebaliknya sulit menemukan suatu bentuk umum yang dapat menghasilkan bilangan prima. Teorema Dirichlet mengatakan terdapat takerhingga banyak bilangan prima yang terdapat didalam barisan aritmatika

$$a, a + b, a + 2b, a + 3b, \cdots$$

asalkan $\gcd(a, b) = 1$. Sebagai contoh, diperhatikan bilangan yang diakhiri oleh angka 999: $1999, 100999, 1000999, \cdots$ merupakan bilangan prima. Mereka ini berbentuk $1000n+999$ dengan $\gcd(1000, 999) = 1$.

Bilangan prima Fermat dan Mersene

Kita fokus pada bilangan bulat yang mempunyai bentuk umum $2^m \pm 1$. Sebagian besar bilangan ini adalah prima, misalnya $3, 5, 7, 13, 31, 127, \cdots$, semuanya berbentuk $2^m \pm 1$. Kita tahu persis bentuk umum m yang membuat bilangan ini prima. Namun sebaliknya kita dapat mendeteksi bentuk m bilamana $2^m + 1$ prima, seperti diungkapkan pada teorema berikut.

Teorema 2.7. *Bila $2^m + 1$ prima maka $m = 2^n$ untuk suatu $n \geq 0$.*

Bukti. Dibuktikan melalui kontraposisinya. Diketahui m tidak berbentuk 2^n. Maka ada bilangan ganjil $q > 1$ sehingga $m = 2^n q$. Alasannya adalah sebagai berikut: untuk q ganjil, katakan $q = 2k + 1$ maka $m = 2^n(2k + 1)$, yaitu diantaranya berbentuk $2^n \cdot 3, 2^n \cdot 5, 2^n \cdot 7, \cdots$ kesemuanya tidak mungkin berbentuk 2^n karena faktor ganjilnya tidak dapat digabungkan dengan 2 untuk membentuk $2^{(\cdot)}$. Bila q genap maka ada kemungkinan $2^n q$ berbentuk $2^{(\cdot)}$, misalnya $2^n \cdot 4 = 2^{n+2}$. Perhatikan polinomial $P(t) = t^q + 1$. Karena q ganjil maka dapat difaktorkan $P(t) = (t + 1)(t^{q-1} - t^{q-2} + \cdots + t^2 - t + 1)$, jadi $(t + 1)$ merupakan faktor dari $P(t)$. Ambil $t = x^{2^n}$, substitusi ke dalam $P(t)$ diperoleh $P\left(x^{2^n}\right) = \left(x^{2^n}\right)^q + 1 = x^{2^n q} + 1 = x^m + 1$ mempunyai faktor $(x^{2^n} + 1)$. Diambil $x = 2$ maka disimpulkan $(2^{2^n} + 1)$ adalah faktor dari $2^m + 1$. Jadi $2^m + 1$ bukan prima. ■

Bilangan yang berbentuk $F_n := 2^{2^n} + 1, n \geq 0$ disebut **bilangan Fermat**. Bilangan Fermat yang merupakan bilangan prima disebut **prima Fermat**. Ada konjektur bahwa semua bilangan Fermat adalah prima. Coba perhatikan beberapa diantaranya $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_5 = 65537$ kesemuanya adalah prima. Namun pada tahun 1732 Euler menunjukkan bahwa bilangan Fermat berikutnya adalah komposit, yaitu

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417,$$

sehingga konjektur tersebut tidak terbukti.

Walaupun tidak semua bilangan Fermat adalah prima, namun dapat dipastikan setiap pasangan dua bilangan Fermat membentuk prima relatif, yaitu $\gcd(F_n, F_{n+k}) = 1$. Untuk bukti, lihat Jones and Jones (2005).

Selanjutnya, bilangan yang berbentuk 2^p+1 dimana p prima disebut **bilangan Mersene**, dan diantara bilangan ini yang prima disebut **bilangan prima Mersene**. Untuk $p = 2, 3, 5, 7$ diperoleh bilangan prima Mersene berikut

$$M_p = 3, 7, 31, 127,$$

tetapi untuk $p = 11$, $M_{11} = 2^{11} + 1 = 2047 = 23 \times 89$ ternyata bukan prima.

2.4 Uji Keterbagian

Berdasarkan Teorema Fundamental Aritmatika kita selalu dapat menyajikan sebarang bilangan bulat dalam bentuk perkalian bilangan prima berpangkat. Permasalahannya adalah bagaimana cara efektif untuk menemukan semua faktor tersebut. Metoda coba-coba sangat tidak efektif terutama bilangannya besar. Untuk itu diperlukan cara untuk mendeteksi awal suatu bilangan bulat dapat terbagi oleh bilangan bulat lainnya.

Suatu bilangan bulat n dalam bentuk desimal dan dalam basis 10 ditulis sebagai berikut

$$n = a_k a_{k-1} \cdots a_1 a_0 \leftrightarrow n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0.$$

Sebagai contoh $n = 3457$ berarti $k = 3$ dan $n = 3 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10^1 + 7$. Berikut beberapa proposisi untuk uji keterbagian.

Proposisi 2.1. *n habis terbagi 2 bila hanya bila a_0 genap.*

Bukti. Cukup jelas.

Proposisi 2.2. *n habis dibagi 3 bila hanya bila jumlah angka-angka pembangunnya habis dibagi 3.*

Bukti. Diperhatikan bentuk $10^k = (9+1)^k$. Bila dijabarkan maka akan menghasilkan bentuk m_k+1 dimana m_k suatu bilangan kelipatan 9, jadi habis dibagi 3. Ilustrasi, $(9+1)^1 = \underbrace{9}_{m_1}+1$, $(9+1)^2 = \underbrace{9^2+2\cdot 9}_{m_2}+1$, $(9+1)^3 = \underbrace{9^3+3\cdot 9^2+3\cdot 9}_{m_3}+1$. Secara umum dijabarkan dengan menggunakan formula binomial

$$(9+1)^k = \sum_{r=0}^{k} \left(\begin{array}{c} k \\ r \end{array} \right) 9^r 1^{k-r} = 1 + \underbrace{\sum_{r=1}^{k} \left(\begin{array}{c} k \\ r \end{array} \right) 9^r}_{m_k}.$$

Jadi diperoleh

$$n = \underbrace{(a_k m_k + a_{k-1} m_{k-1} + \cdots + a_1 m_1)}_{M} + (a_k + a_{k-1} + \cdots + a_1 + a_0).$$

Karena $3|M$ maka diperoleh $3|n \leftrightarrow 3|(a_k + a_{k-1} + \cdots + a_1 + a_0)$. ■

Contoh 2.8. Bilangan 372 habis dibagi 3 sebab $3+7+2 = 12$ habis dibagi 3, tetapi bilangan 4561 tidak dapat dibagi 3 sebab $4+5+6+1 = 16$ tidak terbagi oleh 3, silahkan cek!.

Proposisi 2.3. *n habis dibagi 4 bila hanya bila bilangan yang dibentuk oleh dua digit terakhirnya habis dibagi 4.*

Bukti. Diperhatikan $n = \underbrace{a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2}_{Q} + a_1 10 + a_0$. Karena Q selalu habis dibagi 4 maka n habis dibagi 4 bila hanya bila $a_1 10 + a_0 \equiv a_1 a_0$ habis dibagi 4. ■

Contoh 2.9. Bilangan 4562 tidak habis dibagi 4 sebab 62 tidak habis dibagi 4, sedangkan 34232 habis dibagi 4 sebab32 habis dibagi 4.

Proposisi 2.4. *n habis dibagi 5 bila hanya bila angka terakhirnya 0 atau 5.*

Bukti. Cukup jelas.

Proposisi 2.5. *n habis dibagi 6 bila hanya bila jumlah angka-angka pembangunnya habis dibagi 3 dan angka terakhirnya a_0 genap.*

Bukti. $6|n \leftrightarrow 3|n$ dan $2|n$. Dengan menggunakan Proposisi 2.1 dan 2.1, terbuktilah proposisi ini. ■

Contoh 2.10. Bilangan 6531 dan 47502 kedua habis dibagi 3 sebab jumlah angka-angkanya habis dibagi 3. Selanjutnya, 47502 habis dibagi 6 tetapi 6531 tidak habis dibagi 6.

Catatan 2.1. *Bila habis dibagi 6 maka habis dibagi 3, tetapi tidak berlaku sebaliknya.*

Proposisi 2.6. *Syarat cukup n habis dibagi 7 adalah M habis dibagi 7, dimana M bilangan lebih kecil yang diperoleh dengan cara membuang angka terkahir N kemudian menguranginya dengan 2 kali angka terakhir tersebut.*

Sebelum dibuktikan diperhatikan dulu contoh berikut.

Contoh 2.11. Diperhatikan bilangan $n = 47292$. Kita perkecil bilangan ini dengan menggunakan teknik pada proposisi di atas.

$$47292 \to 4729 - 2(2) = 4725 \to 472 - 2(5) = 462 \to 46 - 2(2) = 42 =: M.$$

Karena M habis dibagi 7 maka disimpulkan n habis dibagi 7. Silahkan cek!

Bukti. Berdasarkan pembentukan M seperti pada proposisi kita dapat menulis

$$\begin{aligned} M &= a_k 10^{k-1} + a_{k-1} 10^{k-2} + \cdots + a_2 10 + a_1 - 2a_0 \\ 10M &= a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 - 2a_0 10 \\ &= \underbrace{a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0}_{n} - a_0 - 20a_0 \\ &= n - 21a_0. \end{aligned}$$

Jadi diperoleh hubungan $n = 10M + 21a_0$. Jelas bila $7|M$ maka $7|n$ sebab $21a_0$ selalu habis dibagi 7. ■

Proposisi 2.7. *n habis dibagi 8 bila hanya bila bilangan yang dibentuk oleh tiga digit terakhirnya habis dibagi 8.*

Bukti. Tulis $n = \underbrace{a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_3 10^3}_{T} + (a_2 10^2 + a_1 10 + a_0)$. Karena T selalu habis dibagi 8 maka n habis dibagi 8 bila hanya bila $a_2 10^2 + a_1 10 + a_0 \equiv a_2 a_1 a_0$ habis dibagi 8. ■

Proposisi 2.8. *n habis dibagi 9 bila hanya bila jumlah angka-angka pembangunnya habis dibagi 9.*

Bukti. Gunakan argumen yang sama ketika membuktikan habis dibagi 3. ■

Proposisi 2.9. *n habis dibagi 10 bila hanya bila angka terakirnya 0.*

Bukti. Cukup jelas. ■

Proposisi 2.10. *n habis dibagi 11 bila hanya bila selisih antara jumlah angka pada urutan genap dan urutan ganjil habis dibagi 11.*

Bukti. Diperhatikan suku $10^i = (11-1)^i = 11q + (-1)^i$. Misalnya $10^1 = 11 - 1$, $10^2 = (11-1)^2 = 11^2 - 2(11) + (-1)^2 = 11\underbrace{(11-2)}_{q} + (-1)^2$, $10^3 = (11-1)^3 = 11^3 - 3(11^2) + 3(11) + (-1)^3 = 11\underbrace{(11^2 - 3(11) + 3)}_{q} + (-1)^3, \cdots$ Jadi diperoleh ekspresi berikut (dengan asumsi k genap):

$$n = 11K + \sum_{i=1}^{k} a_k(-1)^i = 11K + ((a_2 + a_4 + \cdots + a_k) - (a_1 + a_3 + \cdots + a_{k-1}))\,.$$

Karena $11K$ selalu habis dibagi 11 maka diperoleh n habis dibagi 11 bila hanya bila suku $(a_2 + a_4 + \cdots + a_k) - (a_1 + a_3 + \cdots + a_{k-1})$ habis dibagi 11.

Contoh 2.12. Coba periksa apakah 8679 dan 3567811 dapat dibagi oleh 11.

Penyelesaian. Perhatikan bilangan 8679. Selisih jumlah digit pada posisi genap dan ganjil adalah

$$(8+7) - (6+9) = 0$$

ternyata habis dibagi 11. Jadi bilangan 8679 habis dibagi 11. Untuk bilangan 3567811 diperoleh

$$(3+6+8+1) - (5+7+1) = 18 - 13 = 6$$

tidak dapat dibagi 11 sehingga 3567811 juga tidak habis dibagi 11. Coba cek! ■

Contoh 2.13. Temukan semua faktor prima bilangan 510510, kemudian hitung banyak semua faktor positifnya.

Penyelesaian. Sekilas pandang, bilangan ini terbagi oleh 2 (karena angka terakhirnya genap), terbagi oleh 5 (karena angka terakhirnya 0). Hasilnya sementara adalah $510510 = 2 \cdot 5 \cdot 51051$. Karena $5+1+0+5+1 = 12$ terbagi oleh 3 maka 51051 juga terbagi oleh 3, hasil berikutnya adalah $510510 = 2 \cdot 5 \cdot 3 \cdot 17017$. Sekarang fokus pada bilangan 17017. Perhatikan selisih $(1+0+7) - (7+1) = 0$ habis dibagi 11, yaitu $17017 = 11 \times 1547$. Untuk bilangan 1547 diperoleh

$$1547 \to 154 - 2(7) = 140 \to 14 - 2(0) = 14 \to M$$

habis dibagi 7 sehingga 1547 juga habis dibagi 7, yaitu $1547 = 7 \times 221$. Nah, bilangan 221 sudah cukup kecil sehingga dengan mudah difaktorkan sebagai $221 = 11 \cdot 13$. Diperoleh hasil akhir faktorisasi prima sebagai berikut

$$510510 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17.$$

Berdasarkan teori yang sudah dibahas sebelumnya, banyak faktor positif yang ada ditentukan berdasarkan

$$(1+1)(1+1)(1+1)(1+1)(1+1)(1+1)(1+1) = 2^7 = 128. \quad \blacksquare$$

Contoh 2.14. Diberikan bilangan $N = 181920...92939495$, yaitu diperoleh dengan menuliskan secara berurutan digit bilangan dua digit dari 18 sampai dengan 95. Apakah N terbagi habis oleh 3. Jika iya, tentukan pangkat tertinggi p pada faktorisasi prima 3^p.

Penyelesaian. Diamati secara seksama frekuensi kemunculan angka 1 s.d. 9 pada bilangan N, hasilnya diringkas pada tabel berikut

Angka(a)	f	*Muncul pada*	$f \cdot a$
1	10	$18, 19, 21, 31, 41, 51, 61, 71, 81, 91$	10
2	18	$20, 21, 22, \cdots, 29, 32, 42, 52, 62, 72, 82, 92$	36
3	18	$23, 30, \cdots, 33, \cdots, 39, 43, 53, 63, 73, 83, 93$	54
4	18	$24, 34, 40, \cdots, 44, \cdots, 49, 54, 64, 74, 84, 94$	72
5	18	$25, 35, 45, 50, \cdots, 55, \cdots, 59, 65, 75, 85, 95$	90
6	17	$26, 36, 46, 56, 60, \cdots, 66, \cdots, 69, 76, 86$	102
7	17	$27, 37, 47, 57, 67, 70, \cdots, 77, 78, 79, 87$	119
8	18	$18, 28, 38, 48, 58, 68, 78, 80, \cdots, 88, 89$	144
9	14	$19, 29, 39, 49, 59, 69, 79, 89, 90, \cdots, 95$	126
		$\sum$	753

Dengan menggunakan sifat keterbagian 3, diperoleh

$$753 \to 7 + 5 + 3 = 15.$$

Jadi N dapat dibagi 3. Karena 15 hanya terbagi oleh 3 tetapi tidak terbagi oleh 9 maka $p = 1$ adalah pangkat tertinggi pada faktor 3^p. $\blacksquare$