*APOTEMA: Jurnal Pendidikan Matematika.* *Volume 2, Nomor 2 Juli 2016*
*p 63-75. ISSN 2407-8840*

# BILANGAN SEMPURNA GENAP DAN KEPRIMAAN BI LANGAN MERSENNE

**Moh. Affaf**

Prodi Pendidikan Matematika STKIP PGRI BANGKALAN
Email: affafs.theorem@yahoo.com

**abstrak**. Suatu bilangan asli $n$ dikatakan bilangan sempurna jika dan hanya jika jumlah semua pembagi positif dari $n$ selain $n$ adalah $n$. Pada Jamannya, Euler menemukan ciri untuk suatu bilangan genap merupakan bilangan sempurna, yaitu bilangan itu harus mengandung bilangan prima mersenne. Oleh karenanya, dalam pembahasan bilangan sempurna genap diperlukan juga suatu prosedur untuk menyatakan suatu bilangan mersenne prima atau bukan. Untuk mencapai hal tersebut, maka dalam penelitian ini juga dihadirkan suatu prosedur untuk menyatakan suatu bilangan mersenne prima atau bukan. Tes ini dikenal dengan nama Tes Lucas-Lehmer.

**Kata Kunci** : Bilangan Sempurna, Bilangan Sempurna Genap, Bilangan Mersenne, Tes Lucas, Tes Lucas-Lehmer

## PENDAHULUAN

Teorema fundamental dari bilangan bulat menyatakan bahwa setiap bilangan bulat yang lebih dari satu dapat difaktorkan menjadi bilangan-bilangan prima. Teorema ini memiliki arti lain, yaitu setiap bilangan bulat lebih dari satu, pasti memiliki faktor selain bilangan itu sendiri. Kemudian, matematikawan terdahulu tertarik untuk mempelajari hubungan bilangan bulat lebih dari satu dengan faktor-faktor positif yang bukan bilangan itu sendiri. Salah satu diantataranya adalah bilangan sempurna. Suatu bilangan bulat positif dikatakan sempurna jika jumlah semua faktor positif dari bilangan tersebut selain bilangan itu adalah bilangan itu sendiri. Sejak jaman Euclid, bilangan sempurna telah menjadi bahasan yang menarik. Kemudian di jamannya, Euler menemukan ciri khusus bilangan sempurna dalam kasus bilangan tersebut genap, yaitu bilangan tersebut harus memiliki faktor prima Mersenne. Jadi, perlu untuk mengkaji keprimaan bilangan Mersenne jika ingin mempelajari bilangan sempurna genap.

1. Landasan Teori

Pada bagian ini, akan dibahas tentang pembentukan konstruksi $[x, y]$ yang nantinya bisa dijadikan pemrbandingan dengan konstruksi baru yang akan dibentuk pada Hasil dan Pembahasan. Untuk mengawali bagian ini, akan perkenalkan tentang definisi Tripel Pythagoras

### 2.1. Kongruensi bilangan bulat dan sifat-sifat didalamnya

Satu lagi konsep penting dalam teori bilangan adalah kongruensi. Definisi kongruensi bilangan bulat diberikan sebagai berikut.

**Definisi 2.1.1(Kongruen).** Misal $m$ bilangan bulat yang lebih besar dari 1. Bilangan bulat $a$ dan $b$ dikatakan kongruen modulo $m$ dan dituliskan

$a \equiv b(mod\, m)$ jika dan hanya jika $m|a-b$.

**Contoh 2.1.1.**

7 dan 5 kongruen modulo 2 karena $2|(7-5)$

**Teorema 2.1.1.** Misal *a* , *b* , *c* , *d* ,*e* , dan *m* adalah bilangan bulat dengan *d >0* dan *m>0*, maka:

(i) $a \equiv a(mod\, m)$

(ii) jika $a \equiv b(mod\, m)$ maka $b \equiv a(mod\, m)$

(iii) jika $a \equiv b(mod\, m)$ dan $b \equiv c(mod\, m)$ , maka $a \equiv c(mod\, m)$

(iv) jika $a \equiv b(mod\, m)$ dan $d|m$ , maka $a \equiv b(mod\, d)$

(v) jika $a \equiv b(mod\, m)$ dan $c \equiv e(mod\, m)$ , maka $ac \equiv be(mod\, m)$

(vi) jika $a \equiv b(mod\, m)$ dan $c \equiv e(mod\, m)$ , maka $a+c \equiv b+e(mod\, m)$

Bukti:

(i) Jelas bahwa $m|a-a=0$

(ii) $m|a-b$ maka $m|-(a-b)=b-a$

(iii) $m|a-b$ dan $m|b-c$. Tetapi $m|(b-c)+(a-b)=a-c$ menurut Lemma 2.1.1. bagian (ii)

(iv) Karena $d|m$ dan $m|a-b$, maka $d|a-b$ menurut Lemma 2.1.1 bagian (i)

(v) $m|a-b$ dan $m|c-e$. Tetapi $m|(a-b)e+(c-e)a=ac-be$ menurut Lemma 2.1.1. bagian (ii)

(vi) $m|a-b$ dan $m|c-e$, maka $m|(a-b)+(c-e)=(a+c)-(b+e)$

Pada bagian (i) sampai (iii) menyatakan bahwa pada kongruensi berlaku relasi ekivalen yang akan dijelaskan pada bahasan akhir di bab ini. Sedangkan untuk bagian (iv) sampai (vi) akan sering digunakan untuk membuktikan teorema-teorema pada bahasan ini.

**Teorema 2.1.2.** *a* ,*b* , dan *m* bilangan bulat dengan *m >0* sehingga $a \equiv b(mod\, m)$. Maka untuk bilangan bulat positif *n* berlaku $a^n \equiv b^n(mod\, m)$

Bukti:

1. Jelas $S(1)$ benar
2. Jika $S(k)$ benar untuk suatu bilangan positif , berarti $a^k \equiv b^k(mod\, m)$ . Karena $S(1)$ benar , berdasarkan Teorema 2.1.1 bagian (v), maka $aa^k \equiv bb^k(mod\, m)$ , yaitu $a^{k+1} \equiv b^{k+1}(mod\, m)$ . Jadi $S(k+1)$ juga benar.

Berdasarkan Prinsip Induksi Matematika, maka $S(n)$ benar untuk setiap bilangan bulat positif $n$.

**Definisi 2.1.2(residu terkecil).** Jika *m > 0* dan *r* sisa dari pembagian *b* oleh *m*, maka *r* dikatakan residu terkecil dari *b* modulo *m* . Kemudian, dikatakan $\mathbb{Z}_m$ sebagai himpunan semua residu terkecil dari *b* untuk $b \in \mathbb{Z}$, mudah diketahui bahwa $\mathbb{Z}_m = \{0,1,2,\dots,m-1\}$. Serta didefinisikan $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m | (a,m)=1\}$.

**Contoh 2.1.2.**

Untuk *m* = 6, maka $\mathbb{Z}_m^* = \{1,5\}$

**Teorema 2.1.3.** Diberikan bilangan bulat *a, x, y,* dan *m* dengan *m* >0. Jika (*a,m*) = 1 dan $ax \equiv ay(mod\, m)$, maka $x \equiv y(mod\, m)$.

Bukti:

Karena $ax \equiv ay(mod\, m)$, maka $m|(ax-ay)=a(x-y)$, dan berdasarkan teorema 2.1.6 maka $m|(x-y)$, atau dengan kata lain $x \equiv y(mod\, m)$.

**Teorema 2.1.4.** Diberikan bilangan *a* dan *p* dengan *p* prima. Jika $(a,p)=1$, maka $a^{p-1} \equiv 1(mod\, p)$.

Bukti:

Perhatikan himpunan $B = \{1,2,3,\dots,p-1\}$. Jelas bahwa untuk setiap $b_1, b_2 \in B$ dengan $b_1 \neq b_2$ berlaku $b_1 \not\equiv b_2(mod\, p)$. Sekarang,

andai $ab_1 \equiv ab_2(mod\ p)$ untuk $b_1, b_2 \in B$ dengan $b_1 \neq b_2$. Berdasarkan Teorema 2.1.3 berlaku $b_1 \equiv b_2(mod\ p)$. Jadi $ab_1 \not\equiv ab_2(mod\ p)$. Oleh karena itu, untuk $b_1 \in B$ terdapat $b_2 \in B$ dengan $b_1 \neq b_2$ sehingga $ab_1 \equiv b_2(mod\ p)$. Maka diperoleh

$$(a.1)(a.2) \dots (a.(p-1)) \equiv 1.2.1 \dots .(p-1)(mod\ p)$$

$$a^{p-1}.1.2.1 \dots .(p-1) \equiv 1.2.1 \dots .(p-1)(mod\ p)$$

Dengan menerapkan Teorema 2.1.3 diperoleh $a^{p-1} \equiv 1(mod\ p)$

**Teorema 2.1.5 (Teorema Wilson).** Untuk bilangan prima *p* berlaku

$$1.2.1 \dots (p-1) \equiv -1(mod\ p)$$

Bukti:

Sekarang, perhatikan persamaan kongruensi $x^2 \equiv 1(mod\ p)$ untuk suatu bilangan prima *p*. Maka $p|(x^2 - 1) = (x+1)(x-1)$, sehingga $p|(x+1)$ atau $p|(x-1)$ menurut teorema 2.1.9, sehingga $x \equiv -1(mod\ p)$ atau $x \equiv 1(mod\ p)$. Jika solusi persamaan kongruensi $x^2 \equiv 1(mod\ p)$ diambil dalam himpunan

$B = \{1,2,3, \dots, p-1\}$, persamaan tersebut berlaku untuk *x* = 1 atau *x* = p - 1. Untuk $b \in B - \{1, p-1\}$, persamaan kongruensi $bx \equiv 1(mod\ p)$ memiliki solusi berdasarkan Akibat 2.1.1 Jika $b_1 \in B$ adalah solusinya, jelas $b \neq b_1$.

**Definisi 2.1.3.** Untuk bilangan bulat nonnegatif *m* dan *n* dengan $m \geq n$, didefinisikan $\binom{m}{n} = 1$ jika $n = 0$ atau $n = m$; dan $\binom{m}{n} = \frac{m(m-1)(m-2)\dots(m-n+1)}{n!}$ untuk yang lainnya.

**Teorema 2.1.6.** Jika $p$ prima, maka $(a+b)^p \equiv a^p + b^p(mod\ p)$

Bukti:

Telah diketahui bahwa $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$ untuk sebarang bilangan asli *n*. Jadi akan dibuktikan bahwa $p|\binom{p}{m}$ untuk $1 \leq m \leq p-1$. Karena $\binom{p}{m}$ bilangan bulat maka $m!\,|p(p-1)(p-2)\dots(p-n+1)$. Kemudian, karena setiap bilangan asli yang kurang *p* prima relatif dengan *p*, ini artinya, semua hasil kalinya, yaitu $m!$ Juga prima relatif dengan *p* berdasarkan Teorema 2.2.1, sehingga berdasarkan Teorema 2.1.6 $m!\,|(p-1)(p-2)\dots(p-n+1)$, dengan kata lain $\frac{(p-1)(p-2)\dots(p-n+1)}{m!}$ adalah bilangan bulat. Oleh karena itu, $p|\binom{p}{m}$.

## 2.2. Residu Kuadratik

Bahasan ini akan digunakan sebagai dasar pembukrian Tes Lucas dan Tes Lucas-Lehmer yang merupakan tes keprimaan untuk bilangan Mersenne.

**Definisi 2.2.1 (residu kuadratik).** Diberikan bilangan prima *p*. Bilangan bulat *a* dengan $p \nmid a$ disebut residu kuadratik modulo *p* jika dan hanya jika terdapat bilangan bulat *y* sehingga $y^2 \equiv a(mod\ p)$. Jika tidak ada bilangan *y* yang demikian, maka *a* disebut residu nonkuadratik modulo *p*.

**Contoh 2.2.1.**

12 residu kuadratik modulo 13 tetapi 2 residu nonkuadratik modulo 5.

**Definisi 2.2.2(Simbol Legendre).** Misal *p* adalah prima ganjil yang tak membagi bilangan bulat *a*. Didefinisikan $\left(\frac{a}{p}\right) = 1\ atau - 1$ jika dan hanya jika *a* residu kuadratik atau nonkuadratik modulo *a*.

**Contoh 2.2.2.**

Dari Contoh 2.2.1 maka $\left(\frac{12}{13}\right) = 1$ dan $\left(\frac{2}{5}\right) = -1$

**Teorema 2.2.1 (kriteria Euler).** Diberikan bilangan bulat prima ganjil *p* dan $p \nmid a$. Kemudian, jika:

(i) *a* residu kuadratik modulo *p*, maka $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$

(ii) *a* residu nonkuadratik modulo *p*, maka $a^{\frac{p-1}{2}} \equiv -1(mod\ p)$

Bukti:

(i) Karena $\left(\frac{a}{p}\right) = 1$, maka terdapat bilangan bulat *y* sehingga $y^2 \equiv a(mod\ p)$. Tentu saja $p \nmid y$ karena $p \nmid a$, sehingga $a^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1(mod\ p)$

(ii) Karena $\left(\frac{a}{p}\right) = -1$, maka $y^2 \not\equiv a(mod\ p)$ untuk setiap bilangan bulat *y*. Tetapi, selalu terdapat $k, k' \in \{1,2,3, \dots, p-1\}$ sehingga $kk' \equiv a(mod\ p)$. Tentu saja terdapat $(p-1)/2$ pasang $kk'$, oleh karena itu

$$a^{\frac{p-1}{2}} \equiv 1.2.1 \dots (p-1) \equiv -1(mod\ p)$$

**Teorema 2.2.2 (lemma Gauss).** Diberikan bilangan bulat prima ganjil *p* dengan $p \nmid a$. Untuk $x = 1,2,3, \dots, \frac{p-1}{2} = h$, misal $x'$ adalah bilangan bulat kongruen $ax$ modulo *p* dengan $-h \le x' \le h$. Jika banyaknya bilangan $x'$ yang negatif sebanyak *n*, maka $\left(\frac{a}{p}\right) = (-1)^n$

Bukti:

Pertama akan dibuktikan jika $x \neq y$, maka $|x'| \neq |y'|$. Jika $x' = y'$, maka $ax \equiv ay(mod\ p)$ sehingga $x \equiv y(mod\ p)$. Sekarang, jika $x' = -y'$, maka $ax \equiv -ay(mod\ p)$ sehingga $x \equiv -y(mod\ p)$, tentu saja ini juga tidak mungkin. Oleh karena itu, $a^h \prod x = \prod ax \equiv \prod x' \equiv (-1)^n \prod x$, sehingga diperoleh $a^h \equiv (-1)^n (mod\ p)$, atau dengan kata lain $\left(\frac{a}{p}\right) = (-1)^n$

**Teorema 2.2.3.** Diberikan bilangan bulat prima ganjil *p*. Maka $\left(\frac{2}{p}\right) = 1$ jika $p \equiv 1\ atau\ 7(mod\ 8)$ dan $\left(\frac{2}{p}\right) = -1$ jika $p \equiv 3\ atau\ 5(mod\ 8)$.

Bukti:

Dengan memanfaatkan Teorema 2.2.2, maka tinggal mengetahui genap atau ganjil banyaknya $x \in \{1,2, \dots, p-1\}$ yang memenuhi $\frac{p}{2} < 2x < p$, atau bisa dikatakan $\frac{p}{4} < x < \frac{p}{2}$. Misal $p = 4q + r, 0 < r < 4$. Tentu saja $r = 1$ atau $r = 3$ karena $p$ bilangan ganjil, maka $\frac{p}{4} = q + \frac{r}{4} < x < \frac{p}{2} = 2q + \frac{r}{2}$ .

Sekarang jelas bahwa $n = q$ atau $n = q + 1$ bergantung $r = 1$ atau $r = 3$, sehingga

(i) Jika $r = 1$ dan $q = 2s$, maka $p = 8s + 1$ dan $n = q$, yaitu genap

(ii) Jika $r = 1$ dan $q = 2s$+1, maka $p = 8s + 5$ dan $n = q$, yaitu ganjil

(iii) Jika $r = 3$ dan $q = 2s$, maka $p = 8s + 3$ dan $n = q + 1$, yaitu ganjil

(iv) Jika $r = 3$ dan $q = 2s + 1$, maka $p = 8s + 7$ dan $n = q + 1$, yaitu genap

Maka bukti selesai.

**Teorema 2.2.4.** Diberikan bilangan bulat prima ganjil $p > 3$. Maka $\left(\frac{3}{p}\right) = 1$ jika $p \equiv 1\ atau\ 11(mod\ 12)$ dan $\left(\frac{3}{p}\right) = -1$ jika $p \equiv 7\ atau\ 5(mod\ 12)$.

Bukti: Analog dengan bukti Teorema 2.2.3.

**Teorema 2.2.3.** Diberikan bilangan bulat prima ganjil $p > 5$. Maka $\left(\frac{5}{p}\right) = -1$ jika $\equiv 2,7, atau 17(mod\ 20)$ .

Bukti: Analog dengan bukti Teorema 2.2.3.

### 1.3. Grup

**Definisi 2.3.1 (grup).** Diberikan himpunan tak kosong G dengan operasi * yang terdefinisi di G dan dituliskan sebagai $\langle G,* \rangle$. Kemudian, $\langle G,* \rangle$ dikatakan grup jika dan hanya jika memenuhi 4 kondisi berikut:

1. $\forall_{a,b \in G}; a * b \in G$
2. $\forall_{a,b,c \in G}; a * (b * c) = (a * b) * c$
3. $\forall_{a \in G} \ \exists_{e \in G} \ni a * e = e * a = a$. Kemudian *e* disebut elemen identitas di G
4. $\forall_{a \in G} \ \exists_{i \in G} \ni a * i = i * a = e$. Kemudian dikatakan *i* disebut invers dari *a* dan biasanya dituliskan sebagai *–a* atau $a^{-1}$.

Jika $H \subseteq G$ dan $\langle H,* \rangle$ juga membentuk grup, maka dikatakan *H* subgroup *G*.

**Contoh 2.3.1.**

Didefinisikan $\mathbb{Z}_m\sqrt{3} = \{a + b\sqrt{3} | a, b \in \mathbb{Z}_m\}$ serta $+_m$ dan $x_m$ menyatakan operasi jumlah modulo *m* dan operasi kali modulo *m* berturut-turut. Untuk *m* = 3, maka $\mathbb{Z}_m\sqrt{3} = \{0,1,2,\sqrt{3},2\sqrt{3},1+\sqrt{3},1+2\sqrt{3},2+\sqrt{3},2+2\sqrt{3}\}$. Dapat dicek bahwa $\langle \mathbb{Z}_m\sqrt{3}, x_m \rangle$ tidak membentuk grup, tetapi $\langle \mathbb{Z}_m\sqrt{3} - \{0\}, x_m \rangle$ membentuk grup. Kemudian, $\{1\}$ subgroup $\mathbb{Z}_m\sqrt{3} - \{0\}$

**Definisi 2.3.2 (Relasi Ekivalen).** Sebuah relasi ~ pada sebuah himpunan S dikatakan relasi ekivalen jika dan hanya jika untuk setiap $a, b, c \in S$ memenuhi 3 kondisi berikut:

(i) $a \sim a$ (refleksif)
(ii) $a \sim b$ berakibat $b \sim a$ (simetris)
(iii) $a \sim b, b \sim c$ berakibat $a \sim c$ (transitif)

**Contoh 2.3.2.**

Misal S adalah himpunan bilangan bulat dan *n* adalah bilangan bulat yang lebih dari 1 yang telah ditetapkan. Kemudian, didefinisikan $a \sim b$ untuk $a, b \in S$ jika $n|(a-b)$. Tentu saja $a \sim a$ karena $n|0 = a - a$. Jika $a \sim b$, maka
$n|a - b = -(b-a) = -1(b-a)$.
Karena (-1,*n*) = 1, maka $n|(b-a)$. Oleh karena itu $b \sim a$. Jika $a \sim b, b \sim c$, maka $n|(a-b)$ dan $n|(b-c)$. Berdasarkan Lemma 2.1.1 diperoleh $n|(a-b)+(b-c) = (a-c)$. Jadi $a \sim c$. Dengan kata lain pada kongruensi bilangan bulat, berlaku relasi ekivalen. Contoh ini merupakan generalisasi dari "Jika G grup dan H subgroup G, maka $a \sim b$ jika $a, b \in G$, $ab^{-1} \in H$ ". Relasi ini merupakan relasi ekivalen [Herstein. 1990:57].

**Definisi 2.3.3.** Jika ~ adalah relasi ekivalen pada S dan $a \in S$, maka $[a]$, kelas dari $a$ didefinisikan sebagai $[a] = \{b \in S | b \sim a\}$

Pada contoh kutipan di atas, dapat dituliskan $ab^{-1} = h$ untuk suatu $h \in H$. Jadi, $a \sim b$ berakibat $a = hb$. Sekarang, jika $a = kb$ untuk suatu $k \in H$, maka $ab^{-1} = (kb)b^{-1} = k \in H$. Jadi, $a \sim b$ jika dan hanya jika $a \in Hb = \{hb | h \in H\}$, dengan kata lain $[b] = Hb$.

**Teorema 2.3.1.** Jika ~ adalah sebuah relasi ekivalen pada S dan $a \in S$, maka $S = \cup[a]$, gabungan ini berjalan untuk setiap kelas-kelas di S, dan jika $[a] \neq [b]$ berakibat $[a] \cap [b] = \emptyset$

Bukti:

Karena $a \in [a]$, maka tentu saja $\cup_{a \in S}[a] = S$. Sekarang, tinggal membuktikan jika $[a] \neq [b]$ berakibat $[a] \cap [b] = \emptyset$. Berikut akan dibuktikan dengan kontraposisi. Misal $[a] \cap [b] \neq \emptyset$, katakan $c \in [a] \cap [b]$. Berdasarkan kelas, maka $c \sim a$ karena $c \in [a]$ dan $c \sim b$ karena $c \in [b]$. Berdasarkan sifat simetrisnya, $c \sim a$ berakibat $a \sim c$. Karena $a \sim c$ dan $c \sim b$, maka $a \sim b$, maka $a \in [b]$. Sekarang, jika $x \in [a]$, maka $x \sim a$. Tetapi $a \sim b$, oleh karena itu $x \in [b]$. Jadi $[a] \subseteq [b]$. Dengan cara

yang sama, mudah diperoleh $[b] \subseteq [a]$. Jadi $[a] = [b]$, maka bukti teorema selesai.

Teorema ini mengatakan bahwa partisi ini adalah partisi disjoin pada *S*. Teorema ini akan digunakan untuk membuktikan Teorema Lagrange yang merupakan teorema fundamental dalam aljabar abstrak. Namun, sebelum itu, dibutuhkan definisi berikut:

**Definisi 2.3.4.** Diberikan bilangan bulat positif *n* dan grup $\langle G,* \rangle$ dengan $a \in G$. Didefinisikan:

(i) $\circ(G)$ sebagai banyaknya anggota *G*
(ii) $a^n = \underbrace{a * a * a * \ldots * a}_{a\ sebanyak\ n}$
(iii) $\circ(a)$ = *m* dalam kasus *m* bilangan bulat positif terkecil sehingga $a^m = e$, dengan e elemen identitas di *G*.

**Teorema 2.3.2(Teorema Lagrange).** Misal *G* himpunan berhingga dan $H \subseteq G$ sehingga $\langle G,* \rangle$ dan $\langle H,* \rangle$ membentuk grup. Jika $a \in G$, maka:
(i) $\circ(H) | \circ(G)$
(ii) $\circ(a) | \circ(G)$

2. Hasil dan Pembahasan

**Definisi 3.1.** Diberikan $n \in \mathbb{N}$. Jumlah semua pembagi positif dari $n$ dinyatakan dengan $\sigma(n)$.

**Contoh 3.1.**

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$$

**Lemma 3.1.** Diberikan bilangan prima $p$ dan bilangan bulat positif, maka $\sigma(p^n) = \frac{p^{n+1}-1}{p-1}$

Bukti :

$$\sigma(p^n) = 1^{1-1} + p^{2-1} + p^{3-1} + \cdots + p^{(n+1)-1} = \frac{1(p^{n+1}-1)}{p-1} = \frac{p^{n+1}-1}{p-1}$$

menurut Contoh 2.2.1.

**Teorema 3.1.** Jika *a* dan *b* bilangan bulat positif dengan $(a, b) = 1$, maka $\sigma(ab) = \sigma(a)\sigma(b)$

Bukti :

Misal banyak pembagi positif dari *a* adalah *t* dengan $a_1, a_2, a_3, \ldots, a_t$ semua pembaginya dan s banyak pembagi positif dari *b* dengan $b_1, b_2, b_3, \ldots, b_s$, maka $\sigma(a)\sigma(b) = (a_1 + a_2 + a_3 + \cdots + a_t)(b_1 + b_2 + b_3 + \cdots + b_t)$

$$= a_1 b_1 + a_1 b_2 + a_1 b_3 + \ldots + a_1 b_t + a_2 b_1 + a_2 b_2 + a_2 b_3 + \ldots + a_2 b_t \\ \vdots \\ + a_s b_1 + a_s b_2 + a_s b_3 + \ldots + a_s b_t$$

Jika $a_i\ b_j$ dari susunan di atas, maka $a_i\ b_j | ab$ karena $ab = (a_i x_i)(b_j y_j) = (a_i b_j)(x_i y_j)$, dengan kata lain, setiap elemen pada susunan di atas merupakan pembagi positif *ab*. Jika *c* pembagi positif *a* atau *b* jelas *c* muncul dalam susunan di atas. Sekarang, jika *c* bukan pembagi positif *a* dan *b* tetapi *c* pembagi positif *ab*, maka setiap prima pembagi *c* pasti membagi *ab* menurut Lemma 2.2.1. Jadi jika *p* prima dengan $p|c$, maka *p* membagi salah satu dari *a* atau *b*. Karena faktor prima dari *a* dan *b* berbeda , maka elemen pada susunan di atas berbeda dan faktor prima *c* muncul di $a_i$ dan muncul pula di $b_j$ . Dari sini jelas bahwa setiap pembagi positif *ab* muncul dalam susunan di atas. Jadi banyaknya elemen pada susunan di atas sama dengan banyak elemen pembagi positif *ab*, atau $\sigma(a)\sigma(b) = \sigma(ab)$.

**Definisi 3.2.** Bilangan asli $n$ dikatakan *sempurna* jika dan hanya jika jumlah semua pembagi positif yang kurang dari $n$ adalah $n$, yaitu jika $\sigma(n) - n = n$, atau dengan kata lain bilangan asli $n$ *sempurna* jika $\sigma(n) = 2n$

**Contoh 3.2.**

6 merupakan bilangan sempurna karena $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2.6$ tetapi 12 tidak sempurna karena $\sigma(12) = 1 + 2 + 3 + +4 + 6 + 12 = 28 \neq 24 = 2.12$

**Teorema 3.2 (Teorema Euclid).** Jika $n$ bilangan asli sehingga $2^n - 1$ prima, maka bilangan $2^{n-1}(2^n - 1)$ adalah bilangan sempurna.

Bukti :
Jelas bahwa $2^{n-1}$ dan $2^n - 1$ prima relatif sehingga menurut teorema 3.1 berlaku

$$\sigma(2^{n-1}(2^n - 1)) = \sigma(2^{n-1})\sigma(2^n - 1)$$

Dengan menerapkan Lemma 3.1 diperoleh

$$\sigma(2^{n-1}(2^n - 1)) = \left(\frac{2^{(n-1)+1} - 1}{2 - 1}\right)(1 + 2^n - 1)$$
$$= (2^n - 1)2^n$$
$$= \mathbf{2}(2^{n-1}(2^n - 1))$$

Jadi $2^{n-1}(2^n - 1)$ merupakan bilangan sempurna .

**Contoh 3.3.**
$2^2 - 1 = 3$ adalah prima, maka 6 bilangan sempurna karena $6 = 2^{2-1}(2^2 - 1)$.

Pada teorema 3.2 Jelas bahwa bilangan yang dimaksud adalah bilangan genap. Kemudian, pertanyaan yang muncul adalah apakah setiap bilangan genap yang sempurna akan berbentuk $2^{n-1}(2^n - 1)$ dengan $2^n - 1$ prima? Pertanyaan ini dijawab positif oleh Matematikiawan asal Swiss, Leonard Euler dalam

**Teorema 3.3 (Teorema Euler).**

Setiap bilangan genap yang sempurna akan berbentuk $2^{n-1}(2^n - 1)$ dengan $2^n - 1$ adalah prima.
Bukti :
Misal *m* adalah bilangan genap sempurna yang dimaksud, tanpa mengurangi keumuman, dituliskan *m* sebagai $2^k q$ dengan $k > 0$ dan $q$ adalah bilangan ganjil. Maka diperoleh

$$\sigma(m) = \sigma(2^k q) = \sigma(2^k)\sigma(q) = (2^{k+1} - 1)\sigma(q)$$

Tetapi *m* sempurna, yaitu

$$\sigma(m) = \sigma(2^k q) = 2(2^k q) = 2^{k+1}.q$$

Dari 2 hasil di atas, diperoleh $(2^{k+1} - 1)\sigma(q) = 2^{k+1}q$ , atau bisa pula dituliskan $\frac{\sigma(q)}{q} = \frac{2^{k+1}}{2^{k+1}-1}$ . Jelas bahwa $2^{k+1} - 1$ dan $2^{k+1}$ prima relatif. Misal $(\sigma(q), q) = d$, maka $q = d(2^{k+1} - 1) = d.2^{k+1} - d$ dan $\sigma(q) = d.2^{k+1} - d + d = q + d$.
Sekarang, andai $d > 1$, maka $\sigma(q) \geq q + d + 1$ karena $2^{k+1} - 1 > 1$. Hal ini kontadiksi dengan yang diperoleh, yaitu $\sigma(q) = q + d$. Maka haruslah $d = 1$. Jadi, $q = 2^{k+1} - 1$ dan $\sigma(q) = q + 1$, sehingga $q = 2^{k+1} - 1$ adalah prima. Dengan menuliskan $n = k + 1$ maka bukti selesai .

Dari teorema 3.3 jelas bahwa kunci agar suatu bilangan genap untuk sempurna adalah bilangan berbentuk $2^n - 1$ haruslah prima. Jadi, penting untuk mempelajari keprimaan bilangan $2^n - 1$ dalam mempelajari bilangan sempurna genap.

**Definisi 3.3 (Bilangan Mersenne).**
Untuk suatu bilangan bulat positif $k$ , bilangan berbentuk $2^k - 1$ dikatakan bilangan Mersenne ke-*k* dan dituliskan sebagai $M_k$ .

**Contoh 3.4.**
Untuk $k$ = 1 , $M_1 = 1$ dan $k$ = 5 , $M_5 = 31$

**Teorema 3.4.** Jika $M_k$ prima, maka *k* juga prima .
Bukti :
Andai *k* komposit dan $M_k$ prima. Misal $k = ab$. Maka $2^a \equiv 1(mod\ 2^a - 1)$. Kemudian, diperoleh $2^k - 1 \equiv 2^{ab} - 1 \equiv (2^a)^b - 1 \equiv 1 - 1 \equiv 0(mod\ 2^a - 1)$. Berdasarkan definisi kekongruenan, maka $2^a - 1 | 2^k - 1$ . Karena $2^a - 1 > 1$ dan $2^a - 1 \neq 2^k - 1$, ini artinya $2^a - 1$ adalah faktor dari $2^k - 1$ selain 1 dan $2^k - 1$. Hal ini kontradiksi dengan $2^k - 1$ prima. Jadi $2^k - 1$ bilangan prima.

Teorema 3.4 membatasi keprimaan bilangan Mersenne dari segi indeknya. Jadi, jika indek bilangan Mersenne

komposit maka bilangan Mersennenya komposit. Tetapi tidak selalu berlaku bahwa Jika $k$ prima, maka $M_k$ prima. Di jamannya, Euler menemukan faktor bilangan Mersenne dengan indek prima dalam bentuk $4m+3$ untuk $m>1$. Penulis menetapkannya dalam teorema 3.5 berikut.

**Teorema 3.5 (Teorema Euler).** Diberikan bilangan bulat positif $m$ dengan $m>1$ sehingga $k=4m+3$ prima. Jika $2k+1$ prima, Maka $2k+1|M_k$ dan $M_k$ komposit.
Bukti:
Karena $p=2k+1$ prima dan $2k+1\equiv 2(4m+3)+1\equiv 7(mod\ 8)$, maka berdasarkan teorema 2.4.3 diperoleh $\left(\frac{2}{p}\right)=1$, dan berdasarkan Kriteria Euler didapatkan $2^k=2^{\frac{1}{2}(p-1)}\equiv 1(mod\ p)$. Dengan kata lain $p|M_k$. Karena $m>1$, maka $k>3$ dan $M_k>p$, oleh karena itu $M_k$ komposit.

**Contoh 3.5.**
11 adalah bilangan prima dan dapat dituliskan sebagai $11=4.2+3$ . Dan mudah diketahui bahwa $2.11+1=23$ adalah prima. Oleh karena itu, $23|2047=M_{11}$. Jadi $2096128=2^{11-1}(2^{11}-1)$ bukan bilangan sempurna.

**Teorema 3.6 (Tes Lucas).** Diberikan barisan bilangan $r_1,r_2,r_3,...$ dengan $r_1=3$ dan $r_n=r_{n-1}^2-2$ untuk $n\geq 2$. Jika *p* bilangan prima dengan bentuk $4k+3$ untuk suatu bilangan bulat nonnegatif $k$, maka $M_p$ merupakan bilangan prima jika dan hanya jika $r_{p-1}\equiv 0(mod\ M_p)$.
Bukti:

Sebelum membuktikan teorema ini, Penulis akan memberikan klaim untuk 3 kondisi berikut:

(i) klaim bahwa barisan bilangan $r_1,r_2,r_3,...$ dengan sifat di atas ekivalen dengan $r_n=\left(\frac{1+\sqrt{5}}{2}\right)^{2^n}+\left(\frac{1-\sqrt{5}}{2}\right)^{2^n}$ untuk $n\geq 1$.

1. Untuk $n=1$, jelas.
2. Andai $r_n$ benar untuk $n=k$, yaitu $r_k=\left(\frac{1+\sqrt{5}}{2}\right)^{2^k}+\left(\frac{1-\sqrt{5}}{2}\right)^{2^k}$ benar, akan ditunjukkan $r_{k+1}$ juga benar

$$r_{k+1}=\left(\frac{1+\sqrt{5}}{2}\right)^{2^{k+1}}+\left(\frac{1-\sqrt{5}}{2}\right)^{2^{k+1}}$$
$$r_{k+1}=\left(\left(\frac{1+\sqrt{5}}{2}\right)^{2^k}\right)^2+\left(\left(\frac{1-\sqrt{5}}{2}\right)^{2^k}\right)^2$$
$$r_{k+1}=\left(\left(\frac{1+\sqrt{5}}{2}\right)^{2^k}+\left(\frac{1-\sqrt{5}}{2}\right)^{2^k}\right)^2-2\left(\frac{1+\sqrt{5}}{2}\right)^{2^k}\left(\frac{1-\sqrt{5}}{2}\right)^{2^k}$$
$$r_{k+1}=\left(\left(\frac{1+\sqrt{5}}{2}\right)^{2^k}+\left(\frac{1-\sqrt{5}}{2}\right)^{2^k}\right)^2-2(-1)^{2^k}$$
$$r_{k+1}=r_k^2-2=r_{(k+1)-1}^2-2$$

Jadi $r_n=\left(\frac{1+\sqrt{5}}{2}\right)^{2^n}+\left(\frac{1-\sqrt{5}}{2}\right)^{2^n}$ benar untuk semua bilangan asli *n* menurut prinsip Induksi Matematika.

(ii) Klaim bahwa $M_p\equiv 2(mod\ 5)$. Karena $p=4k+3$ dengan *k* bilangan bulat nonnegatif, maka diperoleh

$$M_p=2^{4k+3}-1=8.2^{4k}-1$$
$$=8.16^k-1\equiv 8.1-1$$
$$\equiv 2(mod\ 5)$$

(iii) klaim bahwa $M_p\equiv 7(mod\ 8)$

1. Untuk $n=3$, jelas bahwa $M_3\equiv 7(mod\ 8)$
2. Andai pernyataan benar untuk $n=k$, yaitu $M_k\equiv 7(mod\ 8)$ benar, akan ditunjukkan $M_{k+1}\equiv 7(mod\ 8)$ juga benar

$$M_{k+1}\equiv 2^{k+1}-1(mod\ 8)$$
$$M_{k+1}\equiv 2(2^k+1-1)-1(mod\ 8)$$

$$M_{k+1} \equiv 2(2^k - 1) + 2 - 1 (mod\ 8)$$

$$M_{k+1} \equiv 2.7 + 1 (mod\ 8)$$

$$M_{k+1} \equiv 7 (mod\ 8)$$

Jadi $M_n \equiv 7(mod\ 8)$ benar untuk bilangan asli $n \geq 3$ menurut prinsip Induksi Matematika. Atau boleh dikatakan $M_p \equiv 7(mod\ 8)$ benar untuk bilangan prima ganjil $p = 4k + 3$ untuk suatu bilangan nonnegatif *k*.

(←) Andai $q$ prima sehingga $q|M_p$ dan $r_{p-1} \equiv 0(mod\ M_p)$. Maka $q \leq \lfloor \sqrt{M_p} \rfloor$ menurut Teorema 2.1.2 dan berdasarkan Definisi 2.1.1 diperoleh kesamaan $\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}} + \left(\frac{1-\sqrt{5}}{2}\right)^{2^{p-1}} = sM_p$ untuk suatu $s \in \mathbb{Z}$. Dengan mengalikan kedua ruas dengan $\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}}$, diperoleh

$$\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}} \left(\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}} + \left(\frac{1-\sqrt{5}}{2}\right)^{2^{p-1}}\right) = \left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}} . sM_p$$

$$\left(\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}}\right)^2 + \left(\left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right)\right)^{2^{p-1}} = \left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}} . sM_p$$

$$\left(\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}}\right)^2 + (-1)^{2^{p-1}} = \left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}} . sM_p$$

$$\left(\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}}\right)^2 + 1 = \left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}} . sM_p$$

$$\left(\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}}\right)^2 = \left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}} . sM_p - 1$$

Sekarang, perhatikan grup $\langle \mathbb{Z}_q\sqrt{5} - \{0\}, x_q \rangle$. Mudah diketahui bahwa $\circ(\mathbb{Z}_q\sqrt{5} - \{0\}) = q^2 - 1$. Karena $\left(\frac{1+\sqrt{5}}{2}\right) \in \mathbb{Z}_q\sqrt{5} - \{0\}$, mudah dipahami bahwa $\left(\frac{1+\sqrt{5}}{2}\right)^{2^p} = -1$ di $\mathbb{Z}_q\sqrt{5} - \{0\}$. Dengan mengkuadratkan kedua ruas diperoleh

$$\left(\left(\frac{1+\sqrt{5}}{2}\right)^{2^p}\right)^2 = (-1)^2$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{2.2^p} = 1$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p+1}} = 1$$

di $\mathbb{Z}_q\sqrt{5} - \{0\}$. Jadi order dari $\left(\frac{1+\sqrt{5}}{2}\right)$ adalah $2^{p+1}$. Berdasarkan Teorema 2.5.1 maka $\circ\left(\frac{1+\sqrt{5}}{2}\right) = 2^{p+1} | \circ \left(\mathbb{Z}_q\sqrt{5} - \{0\}\right) = q^2 - 1$, dan menurut Lemma 2.1.1 bagian (iii) diperoleh hasil $2^{p+1} \leq q^2 - 1$. Tetapi $q^2 - 1 \leq 2^p - 2 < 2^{p+1}$, oleh karena itu $q^2 - 1 < 2^{p+1}$. Hal ini kontradiksi dengan $2^{p+1} \leq q^2 - 1$. Jadi, jika $r_{p-1} \equiv 0(mod\ M_p)$ maka $M_p$ prima.

(→) Karena $M_p \equiv 2(mod\ 5)$ dan $M_p \equiv 7(mod\ 8)$, maka $\left(\frac{5}{p}\right) = -1$ dan $\left(\frac{2}{p}\right) = 1$ menurut Teorema 2.4.5 dan Teorema 2.4.3. Kemudian, berdasarkan Kriteria Euler, diperoleh $5^{\frac{M_p-1}{2}} \equiv -1(mod\ M_p)$ dan $2^{\frac{M_p-1}{2}} \equiv 1(mod\ M_p)$. Berdasarkan Teorema 2.3.6 diperoleh $\left(\frac{1+\sqrt{5}}{2}\right)^{M_p} = \frac{1^{M_p}+\sqrt{5}^{M_p}}{2^{M_p}}$ menurut Teorema2.3.6. Kemudian

$$\frac{1^{M_p}+\sqrt{5}^{M_p}}{2^{M_p}} = \frac{1+\sqrt{5}^{M_p}}{2^{M_p}}$$

$$\frac{1^{M_p}+\sqrt{5}^{M_p}}{2^{M_p}} = \frac{1+\left(5^{\frac{M_p-1}{2}}\right)\sqrt{5}}{2.\left(2^{\frac{M_p-1}{2}}\right)^2}$$

$$\frac{1^{M_p}+\sqrt{5}^{M_p}}{2^{M_p}} = \frac{1+(-1)\sqrt{5}}{2.(1)^2}$$

$$\frac{1^{M_p}+\sqrt{5}^{M_p}}{2^{M_p}} = \frac{1-\sqrt{5}}{2}$$

di $\mathbb{Z}_{M_p}\sqrt{5}$. Sehingga

$$\left(\frac{1+\sqrt{5}}{2}\right)^{M_p+1} = \left(\frac{1+\sqrt{5}}{2}\right)^{M_p}\left(\frac{1+\sqrt{5}}{2}\right)$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{M_p+1} = \left(\frac{1-\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}}{2}\right)$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{M_p+1} = -1$$

di $\mathbb{Z}_{M_p}\sqrt{5}$. Dengan mengalikan kedua ruas pada persamaan terkhir dengan $\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}$, diperoleh

$$\left(\frac{1+\sqrt{5}}{2}\right)^{M_p+1}\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}} = -\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}} = -\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}\left(\left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right)\right)^{\frac{M_p+1}{2}} = -\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}(1)^{\frac{M_p+1}{2}} = -\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}.1 = -\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}}$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{M_p+1}{2}} = 0$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}} + \left(\frac{1-\sqrt{5}}{2}\right)^{2^{p-1}} = 0$$

di $\mathbb{Z}_{M_p}\sqrt{5}$. Dengan kata kain, $r_{p-1} \equiv 0(mod\ M_p)$

**Contoh 3.6.**
Untuk $M_7 = 127$. Kemudian, $r_{7-1} = r_6 \equiv 254 \equiv 0(mod\ M_7)$. Jadi $M_7$ prima menurut Tes Lucas.

Teorema 3.4 dan 3.5 sudah cukup baik dalam mengkarakterisasi keprimaan bilangan Mersenne. Kekurangan Teorema 3.4 adalah tak berlaku dua arah dan Teorema 3.5 dan Teorema 3.6 hanya mengkarakterisasi bilangan prima yang kongruen 3 modulo 4 saja. Untuk mengakhiri pembahasan pada skripsi ini, penulis akan menyajikan teorema terakhir yang penulis anggap lebih baik dalam mengkarakterisasi keprimaan bilangan Mersenne. Penulis menempatkannya dalam teorema berikut yang sekaligus merupakan teorema terakhir dalam bab pembahasan ini.

**Teorema 3.7 (Tes Lucas-Lahmer).** Diberikan barisan bilangan $S_1, S_2, S_3, \ldots$ dengan $S_1 = 4$ dan $S_n = S_{n-1}^2 - 2$ untuk $n \geq 2$. Jika $p$ bilangan prima ganjil, $M_p$ merupakan bilangan prima jika dan hanya jika $S_{p-1} \equiv 0(mod\ M_p)$.

Bukti:

Pertama, klaim bahwa barisan bilangan $S_1, S_2, S_3, \ldots$ dengan sifat di atas ekivalen dengan $S_n = \left(2+\sqrt{3}\right)^{2^{n-1}} + \left(2-\sqrt{3}\right)^{2^{n-1}}$ untuk $n \geq 1$.

1. Untuk $n = 1$, jelas.
2. Andai $S_n$ benar untuk $n = k$, yaitu $S_k = \left(2+\sqrt{3}\right)^{2^{k-1}} + \left(2-\sqrt{3}\right)^{2^{k-1}}$ benar, akan ditunjukkan $S_{k+1}$ juga benar

$$S_{k+1} = \left(2+\sqrt{3}\right)^{2^{k+1-1}} + \left(2-\sqrt{3}\right)^{2^{k+1-1}}$$

$$S_{k+1} = \left((2+\sqrt{3})^{2^{k-1}}\right)^2 + \left((2-\sqrt{3})^{2^{k-1}}\right)^2$$

$$S_{k+1} = \left((2+\sqrt{3})^{2^{k-1}} + (2-\sqrt{3})^{2^{k-1}}\right)^2 - 2(2+\sqrt{3})^{2^{k-1}}(2-\sqrt{3})^{2^{k-1}}$$

$$S_{k+1} = \left((2+\sqrt{3})^{2^{k-1}} + (2-\sqrt{3})^{2^{k-1}}\right)^2 - 2(1)^{2^{k-1}}$$

$$S_{k+1} = S_k^2 - 2 = S_{(k+1)-1}^2 - 2$$

Jadi $S_n = (2+\sqrt{3})^{2^{n-1}} + (2-\sqrt{3})^{2^{n-1}}$ benar untuk semua bilangan asli *n* menurut prinsip Induksi Matematika.

(←) Andai $q$ prima sehingga $q|M_p$ dan $S_{p-1} \equiv 0(mod\ M_p)$. Maka $q \leq |M_p|$ menurut Teorema 2.1.2. Karena $S_{p-1} \equiv 0(mod\ M_p)$, maka diperoleh $(2+\sqrt{3})^{2^{p-2}} + (2-\sqrt{3})^{2^{p-2}} = rM_p$ untuk suatu $r \in \mathbb{Z}$. Dengan mengalikan kedua ruas dengan $(2+\sqrt{3})^{2^{p-2}}$, diperoleh

$$(2+\sqrt{3})^{2^{p-2}}\left((2+\sqrt{3})^{2^{p-2}} + (2-\sqrt{3})^{2^{p-2}}\right) = (2+\sqrt{3})^{2^{p-2}}.rM_p$$

$$\left((2+\sqrt{3})^{2^{p-2}}\right)^2 + \left((2+\sqrt{3})(2-\sqrt{3})\right)^{2^{p-2}} = (2+\sqrt{3})^{2^{p-2}}.rM_p$$

$$\left((2+\sqrt{3})^{2^{p-2}}\right)^2 + (1)^{2^{p-2}} = (2+\sqrt{3})^{2^{p-2}}.rM_p$$

$$\left((2+\sqrt{3})^{2^{p-2}}\right)^2 + 1 = (2+\sqrt{3})^{2^{p-2}}.rM_p$$

$$\left((2+\sqrt{3})^{2^{p-2}}\right)^2 = (2+\sqrt{3})^{2^{p-2}}.rM_p - 1$$

Sekarang, perhatikan grup $\langle \mathbb{Z}_q\sqrt{3} - \{0\}, x_q\rangle$. Jelas $\circ(\mathbb{Z}_q\sqrt{3} - \{0\}) = q^2 - 1$. Karena $(2+\sqrt{3}) \in \mathbb{Z}_q\sqrt{3} - \{0\}$, mudah dipahami bahwa $(2+\sqrt{3})^{2^{p-1}} = -1$ di $\mathbb{Z}_q\sqrt{3} - \{0\}$. Dengan mengkuadratkan kedua ruas diperoleh

$$\left((2+\sqrt{3})^{2^{p-1}}\right)^2 = (-1)^2$$

$$(2+\sqrt{3})^{2.2^{p-1}} = 1$$

$$(2+\sqrt{3})^{2^p} = 1$$

di $\mathbb{Z}_q\sqrt{3} - \{0\}$, jadi order dari $(2+\sqrt{3})$ adalah $2^p$. Berdasarkan Teorema 2.5.1 maka $\circ(2+\sqrt{3}) = 2^p | \circ(\mathbb{Z}_q\sqrt{3} - \{0\}) = q^2 - 1$, dan menurut Lemma 2.1.1 bagian (iii) diperoleh hasil $2^p \leq q^2 - 1$. Tetapi $q^2 - 1 \leq 2^p - 2 < 2^p$, oleh karena itu $q^2 - 1 < 2^p$. Hal ini kontradiksi dengan $2^p \leq q^2 - 1$. Jadi, jika $S_{p-1} \equiv 0(mod\ M_p)$ maka $M_p$ prima.

$$M_{k+1} \equiv 2^{k+1} - 1(mod\ 8)$$

$$M_{k+1} \equiv 2(2^k + 1 - 1) - 1(mod\ 8)$$

$$M_{k+1} \equiv 2(2^k - 1) + 2 - 1(mod\ 8)$$

$$M_{k+1} \equiv 2.7 + 1(mod\ 8)$$

$$M_{k+1} \equiv 7(mod\ 8)$$

(→) Terlebih dahulu, akan diklaim $M_p \equiv 7(mod\ 8)$ dan $M_p \equiv 7(mod\ 12)$.

(i) Klaim untuk $M_p \equiv 7(mod\ 8)$

1. Untuk $n = 3$, jelas bahwa $M_3 \equiv 7(mod\ 8)$

2. Andai pernyataan benar untuk $n = k$, yaitu $M_k \equiv 7(mod\ 8)$ benar, akan ditunjukkan $M_{k+1} \equiv 7(mod\ 8)$ juga benar

Jadi $M_n \equiv 7(mod\ 8)$ benar untuk bilangan asli $n \geq 3$ menurut prinsip Induksi Matematika. Atau dengan kata lain, $M_p \equiv 7(mod\ 8)$ benar untuk bilangan prima ganjil *p*.

(ii) Klaim untuk $M_p \equiv 7(mod\ 12)$

Akan dibuktikan $2^{2n+1} - 1 \equiv 7(mod\ 12)$ benar untuk semua bilangan asli $n$.

1. Untuk $n = 1$, jelas bahwa $2^{2(1)+1} - 1 \equiv 7(mod\ 12)$

2. Andai pernyataan benar untuk $n = k$, yaitu

$2^{2k+1} - 1 \equiv 7(mod\ 12)$ benar, akan ditunjukkan $2^{2(k+1)+1} - 1 \equiv 7(mod\ 12)$ juga benar

$$2^{2(k+1)+1} - 1 \equiv 4(2^{2k+1}) - 1(mod\ 12)$$

$$2^{2(k+1)+1} - 1 \equiv 4(2^{2k+1} + 1 - 1) - 1 (mod\ 12)$$

$$2^{2(k+1)+1} - 1 \equiv 4(2^{2k+1} - 1) + 4 - 1 (mod\ 12)$$

$$2^{2(k+1)+1} - 1 \equiv 4.7 + 3 (mod\ 12)$$

$$2^{2(k+1)+1} - 1 \equiv 7 (mod\ 12)$$

Jadi $2^{2n+1} - 1 \equiv 7(mod\ 12)$ benar untuk semua bilangan asli *n* menurut prinsip Induksi Matematika. Atau boleh dikatakan, $M_p \equiv 7(mod\ 12)$ benar untuk bilangan prima ganjil *p*.

Karena $M_p \equiv 7(mod\ 8)$ dan $M_p \equiv 7(mod\ 12)$, maka $\left(\frac{2}{p}\right) = 1$ dan $\left(\frac{3}{p}\right) = -1$ menurut teorema 2.4.3 dan teorema 2.4.4 berturut-turut. Berdasarkan Kriteria Euler, diperoleh $3^{\frac{M_p-1}{2}} \equiv -1(mod\ M_p)$ dan $2^{\frac{M_p-1}{2}} \equiv 1(mod\ M_p)$. Berdasarkan Teorema 2.3.6 diperoleh

$(6 + 2\sqrt{3})^{M_p} \equiv 6^{M_p} + 2^{M_p}\sqrt{3}^{M_p}(mod\ M_p)$. Kemudian

$$6^{M_p} + 2^{M_p}\sqrt{3}^{M_p} = 2.3.\left(2^{\frac{M_p-1}{2}}\right)^2\left(3^{\frac{M_p-1}{2}}\right)^2 + 2.\left(2^{\frac{M_p-1}{2}}\right)^2\left(3^{\frac{M_p-1}{2}}\right)\sqrt{3}$$

$$6^{M_p} + 2^{M_p}\sqrt{3}^{M_p} = 2.3.(1)^2(-1)^2 + 2.(1)^2.(-1)\sqrt{3}$$

$$6^{M_p} + 2^{M_p}\sqrt{3}^{M_p} = (6 - 2\sqrt{3})$$

Jadi $(6 + 2\sqrt{3})^{M_p} \in \mathbb{Z}_{M_p}\sqrt{3}$. Dengan memerhatikan $(2 + \sqrt{3}) = \frac{(6+2\sqrt{3})^2}{24}$, maka

$$(2 + \sqrt{3})^{\frac{M_p+1}{2}} = \left(\frac{(6 + 2\sqrt{3})^2}{24}\right)^{\frac{M_p+1}{2}}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{2}} = \frac{(6 + 2\sqrt{3})^{M_p+1}}{(24)^{\frac{M_p+1}{2}}}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{2}} = \frac{(6 + 2\sqrt{3})^{M_p}(6 + 2\sqrt{3})}{(3.2^3)^{\frac{M_p+1}{2}}}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{2}} = \frac{(6 - 2\sqrt{3})(6 + 2\sqrt{3})}{3^{\frac{M_p+1}{2}}\left(2^{\frac{M_p+1}{2}}\right)^3}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{2}} = \frac{(6 - 2\sqrt{3})(6 + 2\sqrt{3})}{3.\left(3^{\frac{M_p-1}{2}}\right).2^3\left(2^{\frac{M_p-1}{2}}\right)^3}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{2}} = \frac{(6 - 2\sqrt{3})(6 + 2\sqrt{3})}{3.(-1).2^3(1)^3}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{2}} = \frac{24}{-24}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{2}} = -1$$

di $\mathbb{Z}_{M_p}\sqrt{3}$. Dengan mengalikan kedua ruas pada persamaan terakhir dengan $(2 - \sqrt{3})^{\frac{M_p+1}{4}}$, diperoleh

$$(2 + \sqrt{3})^{\frac{M_p+1}{2}}(2 - \sqrt{3})^{\frac{M_p+1}{4}} = -(2 - \sqrt{3})^{\frac{M_p+1}{4}}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{4}}(2 + \sqrt{3})^{\frac{M_p+1}{4}}(2 - \sqrt{3})^{\frac{M_p+1}{4}} = -(2 - \sqrt{3})^{\frac{M_p+1}{4}}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{4}}\left((2 + \sqrt{3})(2 - \sqrt{3})\right)^{\frac{M_p+1}{4}} = -(2 - \sqrt{3})^{\frac{M_p+1}{4}}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{4}}(1)^{\frac{M_p+1}{4}} = -(2 - \sqrt{3})^{\frac{M_p+1}{4}}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{4}}.1 = -(2 - \sqrt{3})^{\frac{M_p+1}{4}}$$

$$(2 + \sqrt{3})^{\frac{M_p+1}{4}} + (2 - \sqrt{3})^{\frac{M_p+1}{4}} = 0$$

$$(2 + \sqrt{3})^{2^{p-2}} + (2 - \sqrt{3})^{2^{p-2}} = 0$$

di $\mathbb{Z}_{M_p}\sqrt{3}$. Dengan kata kain, $S_{p-1} \equiv 0(mod\ M_p)$

**Contoh 3.7.**

1. Untuk $M_7 = 127$. Kemudian, $S_1 = 4$, $S_2 = 4^2 - 2 = 14$, $S_3 = 14^2 - 2 = 194$, $S_4 = 194^2 - 2 \equiv 67^2 - 2(mod\ 127) \equiv 42(mod\ 127)$, $S_5 \equiv 42^2 - 2 \equiv -16(mod\ 127)$ $S_{7-1} \equiv S_6 \equiv (-16)^2 - 2 \equiv 256 - 2 \equiv 254 \equiv 0(mod\ 127)$. Jadi berdasarkan Tes Lucas-Lehmer, $M_7 = 127$ prima. Dengan kata lain, 8128 merupakan bilangan sempurna karena $8128 = 2^{7-1}(2^7 - 1)$ dan $2^7 - 1$ bilangan prima.
2. Untuk $M_{11} = 2047$. Kemudian $S_1 = 4$, $S_2 = 4^2 - 2 = 14$, $S_3 = 14^2 - 2 = 194$, $S_4 = 194^2 - 2 = 37634 \equiv 788(mod\ 2047)$, $S_5 \equiv 788^2 - 2 \equiv 620942 \equiv 701(mod\ 2047)$, $S_6 \equiv 701^2 - 2 \equiv 491399 \equiv 119(mod\ 2047)$, $S_7 \equiv 119^2 - 2 \equiv 14159 \equiv -170(mod\ 2047)$, $S_8 \equiv 170^2 - 2 \equiv 28898 \equiv 240(mod\ 2047)$, $S_9 \equiv 240^2 - 2 \equiv 57598 \equiv 282(mod\ 2047)$, $S_{11-1} \equiv S_{10} \equiv 282^2 - 2 \equiv 79522 \equiv 1736 \not\equiv 0(mod\ 2047)$. Jadi berdasarkan Tes Lucas-Lehmer, $M_{11} = 2047$ prima. Hal ini telah dijelaskan dalam Contoh 3.5 yang juga menyatakan 23 adalah salah satu faktor dari $M_{11}$

## KESIMPULAN

Penelitian ini telah berhasil mengidentifikasi bilamana suatu bilangan genap merupakan bilangan sempurna atau bukan, yaitu bilangan tersebut harus berbentuk $2^{n-1}(2^n - 1)$ dengan $2^n - 1$ adalah bilangan mersenne ke-$n$ yang harus merupakan bilangan prima. Selanjutnya, untuk mengetahui $2^n - 1$ merupakan bilangan prima atau bukan, dapat dicek dengan melakukan Tes Lucas-Lehmer, yaitu saat diberikan barisan bilangan $S_1, S_2, S_3, \ldots$ dengan $S_1 = 4$ dan $S_n = S_{n-1}^2 - 2$ untuk $n \geq 2$. Jika $p$ bilangan prima ganjil, $M_p$ merupakan bilangan prima jika dan hanya jika $S_{p-1} \equiv 0(mod\ M_p)$.

Adapun saran penelitian ke depannya, bisa dilakukan penelitian untuk mengidentifikasi bilangan sempurna ganjil. Penelitian terakhir menyatakan bahwa tidak ada bilangan sempurna ganjil yang kurang dari $3^{500}$. Selain itu, dapat pula dilakukan penelitian untuk memodifikasi Tes Lucas-lehmer agar lebih sederhana, baik dalam bukti maupun prosedurnya.

3. Daftar Pustaka


[1] Khosy, Thomas. 2007. *Elementary number theory with applications*. Amsterdam. Elsivier

[2] J. W. Bruce. 1993. *A Really Trivial Proof of Lucas-Lehmer Test*. Math Montly. Amer.

[3] M, I, Rosen. 1988. *A Proof of Lucas-Lehmer Test*. Math Montly. Amer.

[4] I, R, Herstein. Abstract Algebra. 1999. Jon Wiley and Son. New York

[5] Kravist, Sidney. 2011. *The Lucas-Lehmer Test For Mersenne Numbers*. Dover. New Jersey.

[6] Jaroma, John, H. *Note On The Lucas-Lehmer Test*. Irish Math Society, pg 63 – 72, 2004.

[7] Jaroma, John, H. *Equivalence of pepin's Test and Lucas-Lehmer Test*. European Journal of Pure and Applied Mathematics, Vol 2, No 3, pg 352 – 360, 2009.