KESETARAAN UJI PEPIN DAN LUCAS-LEHMER

Yulismansyah [1*], Sri Gemawati [2], Musraini M [2]

[1] **Mahasiswa Program Studi S1 Matematika**
[2] **Dosen Jurusan Matematika**
Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Riau
Kampus Binawidya Pekanbaru (28293), Indonesia

[*] yulismansyah_matematika08@yahoo.com

ABSTRACT

Pepin test provides a necessary and sufficient condition for a Fermat number to be a prime. Lucas-Lehmer test provides a necessary and sufficient condition for a Mersenne number to be a prime. In this article, we review a part of the work of Jaroma [European Journal of Pure and Applied Mathematics Vol. 2, No. 3, 2009, (352-360)] that is the equivalence structure of Pepin test and Lucas-Lehmer test through Lehmer sequences so that both test can be used to check when a Fermat number or a Mersenne number to be a prime.

Keywords: *Prime numbers, primality, Lehmer sequence, Pepin test, Lucas-Lehmer test.*

ABSTRAK

Uji Pepin memberikan syarat perlu dan cukup agar suatu bilangan Fermat merupakan bilangan prima, sementara uji Lucas-Lehmer memberikan syarat perlu dan cukup agar bilangan Mersenne merupakan bilangan prima. Tulisan ini merupakan *review* sebagian dari tulisan Jaroma [European Journal of Pure and Applied Mathematics Vol. 2, No. 3, 2009, (352-360)] yang berisikan kesetaraan antara uji Pepin dan uji Lucas-Lehmer melalui barisan Lehmer sekawan sehingga kedua uji ini dapat digunakan untuk menentukan kapan sebuah bilangan Fermat atau bilangan Mersenne merupakan bilangan prima.

Kata Kunci: *Bilangan prima, uji primalitas, barisan Lehmer, uji Pepin, uji Lucas-Lehmer.*

1. PENDAHULUAN

Bilangan prima merupakan salah satu materi penting pada bidang teori bilangan sebagai elemen himpunan bagian dari himpunan bulat positif. Bilangan prima adalah bilangan bulat positif $n > 1$ yang hanya memiliki dua faktor yaitu satu dan bilangan itu sendiri. Sebagai contoh yaitu Pierre de Fermat (1601-1665) dengan bilangan Fermat dan Marin Mersenne (1588-1648) dengan bilangan Mersenne [1, h. 225-236], [11, h. 71-76], [14, h. 135-137].

Bilangan Fermat adalah bilangan bulat dalam bentuk $F_n = 2^{2^n} + 1$, dimana $n \geq 0$. Untuk menghormati Pierre de Fermat (1601-1665) yang sangat yakin bahwa bilangan tersebut selalu prima, bilangan tersebut diberi nama bilangan Fermat. Pada tahun 1732, Leonhard Euler menyatakan kekurangan dari pernyataan Fermat dengan pemfaktoran F_5, kemudian pada tahun 1880 F. Landry menunjukkan F_6 bukan bilangan prima dan pada awal tahun 1970 F. Landry menunjukkan F_7 bukan merupakan bilangan prima, sehingga dugaan diperoleh tidak ada bilangan prima Fermat di atas n = 4 kemudian sebuah syarat perlu dan cukup untuk pengujian bilangan prima dari setiap bilangan Fermat disediakan oleh uji Pepin yang disebut juga Fr. Théophile Pepin (1826-1904) [1, h. 225-236], [14, h. 135-137].

Bilangan Mersenne merupakan bilangan bulat dengan bentuk $M_n = 2^n - 1$, dimana $n \geq 1$. Marin Mersenne (1588-1648) menyatakan bilangan tersebut prima untuk $n \in \{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$ dan komposit untuk semua bilangan selain dari $n \leq 257$. Diperlukan waktu lebih dari 300 tahun bagi matematikawan untuk membuktikan dugaan tersebut mempunyai kekurangan dan Mersenne telah membuat beberapa kesalahan. Untuk itu uji Lucas-Lehmer menyediakan syarat perlu dan cukup untuk bilangan Mersenne yang merupakan bilangan prima [1, h. 225-236], [13].

Meskipun tidak ada pernyataan konkrit, baik uji Pepin dan Lucas-Lehmer merupakan pengujian bilangan prima yang secara inheren berasal dari sifat-sifat barisan Lehmer dan kedua uji tersebut dapat dibuktikan dengan argumen yang sama.Kesamaan antara kedua uji primalitas ini tampaknya telah diabaikan. Misalnya, uji Pepin yang pembahasan uji primalitasnya dilakukan berdasarkan barisan Lucas. Selanjutnya, Uji Pepin tidak pernah secara eksplisit disebutkan dalam makalah Lehmer. Selain itu, Williams dalam [15, h. 173] menyebutkan bahwa Pepin telah menyadari bahwa versi sebelumnya dapat diubah menjadi seperti uji Lucas. Namun, hubungan langsung ke hasil Lucas-Lehmer tidak muncul untuk diberikan pada [4], [11, h. 71-76]. Sehingga pembahasan ini bermaksud untuk membuat struktur umum yang setara dari dua uji ini agar dapat dikenal lebih luas.

Pembahasan dimulai dengan memperkenalkan barisan Lehmer. Kemudian dilanjutkan beberapa sifat-sifat barisan Lehmer yang diperlukan. Kemudian dilanjutkan memperkenalkan uji Pepin dan Lucas-Lehmer dalam konteks sejarahnya. Pada bagian terakhir membahas bentuk setara antara uji Pepin dan Lucas-Lehmer yang sama-sama berasal dari barisan Lehmer.

2. BARISAN LEHMER

Pada bagian ini memperkenalkan barisan Lehmer dan barisan Lehmer sekawan. Berdasarkan [4], misalkan R dan Q bilangan bulat relatif prima sehingga barisan Lehmer $\{U_n(\sqrt{R}, Q)\}$ dan barisan Lehmer sekawan $\{V_n(\sqrt{R}, Q)\}$ didefinisikan masing-masing dengan

$$U_{n+2}(\sqrt{R}, Q) = \sqrt{R}U_{n+2} - QU_n,\ U_0 = 0,\ U_1 = 1,\ n \in \{0, 1, \dots\}, \quad (1)$$

dan

$$V_{n+2}(\sqrt{R}, Q) = \sqrt{R}V_{n+2} - QV_n,\ V_0 = 2,\ V_1 = \sqrt{R},\ n \in \{0, 1, \dots\}. \quad (2)$$

Selain itu, karena (1) dan (2) adalah fungsi linear, maka ada solusi dan diberikan secara eksplisit dengan (3) dan (4), masing-masing

$$U_n\left(\sqrt{R},Q\right)=\frac{\theta^n-\phi^n}{\theta-\phi},\ n\in\{0,1,\dots\}, \tag{3}$$

dan

$$V_n\left(\sqrt{R},Q\right)=\theta^n+\phi^n,\ n\in\{0,1,\dots\}, \tag{4}$$

dimana, $\theta=\frac{\sqrt{R}+\sqrt{R-4Q}}{2}$ dan $\phi=\frac{\sqrt{R}-\sqrt{R-4Q}}{2}$.

3. SIFAT-SIFAT DARI BARISAN LEHMER

Berikut Lema-Lema yang memuat sifat-sifat pembagi pada barisan Lucas-Lehmer. Lema 1 menyatakan bahwa tidak ada bilangan prima ganjil yang menjadi faktor dari barisan Lehmer $U_n\left(\sqrt{R},Q\right)$ dan barisan Lehmer sekawan $V_n\left(\sqrt{R},Q\right)$.

Lema 1 [4, h. 421] Faktor persekutuan terbesar dari $U_n\left(\sqrt{R},Q\right)$ dan $V_n\left(\sqrt{R},Q\right)$ adalah 1 atau 2.

Misalkan p bilangan prima ganjil dan $p\nmid a$, maka *Legendre Symbol* $\left(a/p\right)$ didefinisikan 1 untuk a sisa kuadratis modulo $p$dan -1 jika a non sisa kuadratis modulo. Untuk semua a dimana $(a, p) = 1$, a disebut sisa kuadratis modulo p jika kongruensi $x^2\equiv a\pmod p$mempunyai solusi. Sebaliknya, a disebut non sisa kuadratis jika tidak mempunyai solusi. Jika $p\mid a$ maka $\left(a/p\right)=0$. Pertimbangkan *Legendre Symbol* [4] digunakan untuk menunjukkan

$$\sigma=\left(\frac{R}{p}\right),\tau=\left(\frac{Q}{p}\right),\text{ dan }\varepsilon=\left(\frac{\Delta}{p}\right), \tag{5}$$

dimana $\Delta=R-4Q$ dari persamaan karakteristik (1) dan (2). Lema berikut menunjukkan bahwa p harus membagi $U_{p-1}\left(\sqrt{R},Q\right)$ atau $U_{p+1}\left(\sqrt{R},Q\right)$.

Lema 2 [4, h. 423] Misalkan $p\nmid RQ$ maka $U_{p-\varepsilon}\left(\sqrt{R},Q\right)\equiv 0\pmod p$.

Misalkan $\omega(p)=$*rank of apparition* dari p pada $\left\{U_n\left(\sqrt{R},Q\right)\right\}$. Lema 3 menunjukkan bahwa indeks pada barisan Lehmer merupakan kelipatan ω yaitu harus p sebagai faktor.

Lema 3 [4, h. 423] Misalkan ω dinotasikan sebagai *Rank of Apparition* (RoA) dari p dalam barisan $\left\{U_n\left(\sqrt{R},Q\right)\right\}$ maka $p\mid U_n\left(\sqrt{R},Q\right)$ jika dan hanya jika $n=k\omega$, dimana $k\in\{1,2,\cdots\}$.

Lema berikut merupakan pengembangan tulisan dari R. D. Charmichael [2] dimana secara khusus diberikan RoA dari p pada barisan Lehmer $U_n\left(\sqrt{R},Q\right)$, kesamaannya apakah p mempunyai RoA atau tidak pada barisan sekawan $V_n\left(\sqrt{R},Q\right)$. Jika $\omega(p)$ ganjil maka p membagi tak terhingga banyaknya indeks yang dapat diidentifikasi dari

$V_n\left(\sqrt{R},Q\right)$. Sebaliknya, tidak ada indeks dari $V_n\left(\sqrt{R},Q\right)$ yang mungkin berisi *p* sebagai faktor.

Lema 4 [4, h. 424] Jika ω ganjil maka $p \nmid V_n\left(\sqrt{R},Q\right)$. Jika ω genap $(2k)$ maka $p \mid V_{(2n+1)k}$ sehingga tidak ada faktor pembagi selain *p* pada barisan tersebut.

Lema 2 memberikan kondisi dimana *p* membagi $U_{p-1}\left(\sqrt{R},Q\right)$ atau $U_{p+1}\left(\sqrt{R},Q\right)$. Jadi, dapat disimpulkan bahwa RoA dari *p* dimana $p \nmid RQ$ tidak hanya berada di $\left\{U_n\left(\sqrt{R},Q\right)\right\}$ tetapi juga tidak bisa lebih besar daripada $p \pm 1$ sehingga $p \mid U_{(p-\varepsilon)/2}\left(\sqrt{R},Q\right)$.

Lema 5 [4, h. 423] Misalkan $p \nmid RQ\Delta$ maka $U_{\frac{p-\varepsilon}{2}}\left(\sqrt{R},Q\right) \equiv 0 \pmod{p}$ jika dan hanya $\sigma = \tau$, dimana $\tau = (Q/p)$.

Terakhir, Lema 6 menjelaskan kondisi pada indeks dari RoA suatu bilangan *N* merupakan bilangan prima.

Lema 6 [4, h. 442] Jika $N \pm 1$ RoA dari *N* maka *N* prima.

4. UJI PEPIN DAN LUCAS-LEHMER

Untuk memperoleh pemahaman yang lebih lengkap dari kedua uji, akan dibandingkan keduanya terlebih dahulu dalam konteks sejarah. Pada tahun 1877, Fr. Pepin merumuskan Teorema sebagai berikut:

Teorema 1 (Uji Pepin) [8, h. 329] Bilangan bulat $F_n = 2^{2^n} + 1$ dimana *n*> 1 adalah bilangan prima jika dan hanya jika

$$5^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Bukti.

Bilangan F_n orde 2 yang merupakan kuadrat non-sisa dari reprositas 5, dimana *n*> 1. Akan ditunjukkan F_n adalah prima dengan kongruensi $x^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ jika F_n prima maka akan membagi bilangan dari kongruensi tersebut dengan $x = 5$ yaitu $5^{\frac{F_n-1}{2}} + 1$.

Kondisi yang cukup untuk membuktikannya adalah pembagi bilangan prima F_n sama dengan F_n sendiri. Sehingga dengan memisalkan *P* pembagi bilangan F_n dapat dihipotesa dengan kongruensi berikut

$$5^{\frac{F_n-1}{2}}+1\equiv 0,\ 5^{F_n-1}\equiv 1 \pmod{P}. \quad (6)$$

Berdasarkan Teorema Fermat, diperoleh

$$5^{P-1}\equiv 1 \pmod{P}. \quad (7)$$

Faktor pembagi terbesar dari $P-1$ dan F_n-1 adalah perpangkatan 2 dilambangkan dengan 2^{α}. Berdasarkan kongruensi (6) dan (7) dapat disimpulkan menjadi $5^{2^{\alpha}}\equiv 1 \pmod{P}$ dimana $2^{\alpha}<F_n-1$. Pada hipotesis ini, karena 2^{α} merupakan pembagi dari $\frac{F_n-1}{2}$ maka $5^{\frac{F_n-1}{2}}\equiv 1 \pmod{P}$ sehingga akan didapatkan dua kongruensi

$$5^{\frac{F_n-1}{2}}+1\equiv 0 \text{ dan } 5^{\frac{F_n-1}{2}}-1\equiv 0 \pmod{P},$$

yang jelas tidak mungkin. Perpangkatan 2^{α} faktor pembagi terbesar dari $P-1$ dan F_n-1 adalah F_n-1 itu sendiri serta P merupakan pembagi F_n. Syarat perlu $P=F_n$ yang artinya F_n tidak lain faktor prima dirinya sendiri. Sehingga kongruensi (7) dapat menyimpulkan bahwa F_n adalah bilangan prima. □

Pepin didalam tulisannya [8] menyatakan bilangan 10 dapat digunakan di tempat 5. Selanjutnya dikaji ulang oleh François Proth (1852 - 1879) menulis pada tahun 1876 yang kemudian dilanjutkan pada tahun 1878 bahwa dapat menggunakan bilangan 3 sebagai pengganti dari 5 pada Teorema 1 [9], [10], tetapi tak ada bukti dari pernyataannya. Kemudian, Édouard Lucas (1842 - 1891) berpendapat bahwa sebarang bilangan bulat *a* dapat digunakan di tempat 5 asalkan *Jacobi Symbol* (a/F_n) memiliki nilai sama dengan -1 [6] dan pada tahun 1879 dapat dibuktikan [7]. Hasilnya sekarang uji Pepin yang merupakan saran Proth dan dibuktikan oleh Lucas. Penjelasan lebih detail terdapat dalam [16, h. 173]. Sebuah versi modern dari uji Pepin yang diberikan sebagai berikut:

Teorema 2 (Uji Pepin) [8, h. 329-331] Bilangan Fermat $F_n = 2^{2^n}+1$ dimana $n\geq 1$ adalah bilangan prima jika dan hanya jika

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Bukti.

Asumsikan $3^{\frac{(F_n-1)}{2}}\equiv -1 \pmod{F_n}$ maka $3^{(F_n-1)}\equiv 1 \pmod{F_n}$, sehingga orde perkalian 3 modulo F_n membagi $F_n-1=2^{2^n}$ yang merupakan perpangkatan 2. Namun, orde tersebut tidak membagi $\frac{F_n-1}{2}$ dan haruslah sama dengan F_n-1 yang mana terdapat setidaknya bilangan komposit di F_n, maka hal ini terjadi jika dan hanya jika F_n bilangan prima. Syarat perlu asumsikan bahwa F_n bilangan prima. Maka menggunakan kriteria Euler menjadi

$$3^{\frac{(F_n-1)}{2}}\equiv\left(\frac{3}{F_n}\right) \pmod{F_n},$$

dimana $\left(\frac{3}{F_n}\right)$ merupakan *Legendre Symbol*. Dengan pengulangan pengakaran, didapatkan $2^{2^n} \equiv 1 \pmod 3$, sehingga $F_n \equiv 2 \pmod 3$ dan $\left(\frac{F_n}{3}\right) \equiv -1$ berasal dari $F_n \equiv 1 \pmod 4$ yang merupakan aturan resiprositas kuadrat. □

Selanjutnya pengujian primalitas bilangan Mersenne berikut ini diprakarsai oleh Lucas pada tahun 1878. Lucas mengusulkan dua uji untuk menentukan apakah $2^n - 1$ adalah bilangan prima [6] dengan memberikan syarat perlu dan cukup. Pada tahun 1930, D. H. Lehmer menulis bahwa pada jurnal Lucas kondisi untuk uji primalitas cukup tetapi bukan yang diperlukan. Satu yang tidak pasti apakah uji Lucas akan mengungkapkan karakter dari bilangan prima yang sebenarnya atau tidak [4]. Lehmer selanjutnya menulis bahwa RD Carmichael [2] telah memberikan satu himpunan dengan kondisi perlu dan cukup untuk uji primalitas bilangan tersebut. Namun, dengan pengecualian dari dua kasus, mereka bergantung pada keberadaan sepasang penambahan bilangan yang digunakan dalam pengujian bilangan bulat yang diberikan. Jadi, menurut Lehmer, dari sudut pandang praktis melihat uji ini tidak berlaku karena tidak ada metode yang diberikan untuk menentukan bentuk umum pasangan bilangan yang sesuai. Akhirnya, Lehmer menanggapi pengamatannya dengan membentuk kondisi perlu dan cukup eksplisit untuk bilangan Mersenne merupakan bilangan prima [4]. Saat ini umumnya dikenal sebagai uji Lucas-Lehmer.

Pernyataan asli dari hasil ini diapresiasi dan ditemukan dalam [4], meskipun pernah keliru dicatat pada [14] bahwa bukti asli Lehmer tentang uji Lucas-Lehmer diberikan.

Teorema 3 (Uji Lucas-Lehmer) [6, h. 162] Bilangan Mersenne $M_p = 2^p - 1$, adalah bilangan prima jika dan hanya jika membagi $(p-1)st$ dengan barisan

4, 14, 194, 37634, 1416317954,. . .S_n, . . . dimana $S_n = S_{n-1}^2 - 2$.

Sebelum Teorema 3 dibuktikan, diberikan barisan S_n dan Lema yang diperlukan. Misalkan akar dari barisan S_n sebagai berikut:

$$\tau = \tfrac{1+\sqrt{3}}{\sqrt{2}},\ \bar{\tau} = \tfrac{1-\sqrt{3}}{\sqrt{2}},\ \omega = \tau^2 = 2+\sqrt{3} \text{ dan } \bar{\omega} = \tau^2 = 2-\sqrt{3},$$

dimana $\tau\bar{\tau} = -1$ dan $\omega\bar{\omega}$ beberapa Lema untuk membuktikan Teorema 3 dimana S_n merupakan barisan yang berasal dari barisan Lucas.

Lema 7 [14, h. 855] Misalkan *m* bilangan bulat maka $S_m = \omega^{2^{m-1}} + \bar{\omega}^{2^{m-1}}$.

Bukti.

Misalkan $T_m = \omega^{2^{m-1}} + \bar{\omega}^{2^{m-1}}$, maka $T_1 = \omega + \bar{\omega} = 4 = S_1$ dan $T_{m+1} = T_m^2 - 2$. Dengan demikian $T_m = S_m$ untuk setiap *m*.□

Lema 8 [14, h. 856] Jika M_p prima maka $\tau^{M_p+1} \equiv -1 \pmod{M_p}$.

Bukti.
Kongruensi berada di ring dari bilangan bulat aljabar. Tetapkan $q = M_p$, selanjutnya tulis $\sqrt{2}\tau = 1+\sqrt{3}$, pangkatkan kedua sisi dengan pangkat ke-q dan ambil kongruensi modulo q, sehingga $\tau^q 2^{(q-1)/2}\sqrt{2} \equiv 1+3^{(q-1)/2}\sqrt{3} \pmod{q}$ karena $q \equiv -1 \pmod{8}$ maka $2^{(q-1)/2} \equiv (2/q) \equiv 1 \pmod{q}$. Selanjutnya karena $q \equiv 1 \pmod{3}$ maka

$$3^{(q-1)/2} \equiv (3/q) \equiv -1 \pmod{q},$$

sehingga dengan mengikuti hal tersebut akan didapatkan $\tau^q \equiv \bar{\tau} \pmod{q}$ dan $\tau^{q+1} \equiv \tau\bar{\tau} \equiv -1 \pmod{q}$.□

Untuk membuktikan Teorema 3, pertama akan dibuktikan bahwa $S_{p-1} \equiv 0 \pmod{M_p}$ dengan M_p prima. Berdasarkan Lema 7 dengan kondisi $S_{p-1} \equiv 0 \pmod{M_p}$ maka $\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}$ sehingga $\omega^{2^{p-1}} \equiv -1 \pmod{M_p}$ dan $\omega^{2^p} \equiv 1 \pmod{M_p}$.

Misalkan l adalah bilangan prima membagi M_p, grup $G = Z[\sqrt{3}]$. Koset ω berada di (G/lG) mempunyai orde 2^p dengan kongruensi di atas. Jika l terbagi-bagi di G maka tentulah $(G/lG)^* = (Z/lZ)^* \times (Z/lZ)^*$, dan juga 2^p membagi $l-1$. Dengan demikian $l = 1+2^p k$ untuk $k \geq 1$. Ini memungkinkan karena berarti $l \geq 1+2^p > M_p$.

Asumsikan l prima di G maka $(G/lG)^*$ mempunyai orde l^2-1 dan 2^p membagi $l^2-1 = (l-1)(l+1)$. Jika $l \equiv 1 \pmod{4}$ maka haruslah 2^{p-2} membagi $l-1$ atau $l = 1+2^{p-1}k$ untuk $k \geq 1$. Hal tersebut jika akan terjadi karena $2l \geq 2+2^p > M_p$. Jika $l \equiv 3 \pmod{4}$ maka 2^{p-1} membagi $l+1$ sehingga $l \equiv -1+2^{p-1}k$ untuk $k \geq 1$. Satu yang tidak didapatkan $k = 1$ karena $2^{p-1}-1$ tidak membagi 2^p-1. Kasus ini hanya terjadi jika $k = 2$ sehingga $l = 2^p - 1 = M_p$ dimana M_p bilangan prima. Terakhir, asumsikan M_p bilangan prima. Berdasarkan Lema 8 akan didapat

$$\tau^{M_p+1} \equiv -1 \pmod{M_p} \text{ atau } \tau^{2^p} + 1 \equiv 0 \pmod{M_p}.$$

Karena $\tau^2 = \omega$ maka $\omega^{2^{p-1}} + 1 \equiv 0 \pmod{M_p}$. Kalikan kedua sisi kongruensi dengan $\bar{\omega}^{2^{p-2}}$ dimana $\omega\bar{\omega} = 1$ sehingga $S_{p-1} = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}$. □

5. KESETARAAN UJI PEPIN DAN LUCAS-LEHMER

Pada bagian ini akan ditunjukkan bahwa uji Pepin dan Lucas-Lehmer mempunyai struktur setara, yaitu pada bentuk syarat perlu dan cukup dari kedua uji tersebut. Bentuk $3^n + 1$dari uji Pepin pada Teorema 2 dan bentuk barisan $S_n = S_{n-1}^2 - 2$ dari uji Lucas-Lehmer pada Teorema 3 sama-sama berasal dari barisan Lehmer sekawan $V_n(\sqrt{R}, Q)$.

Untuk itu, selanjutnya akan diselidiki bahwa barisan Lehmer $\{V_n(4,3)\} = 3^n + 1$ melalui Teorema berikut.

Teorema 4 [3, h. 358] Ambil sebarang bilangan bulat. Selanjutnya barisan Lehmer Sekawan $\{V_n(\sqrt{R}, Q)\} = \{V_n(a+1, a)\}$ membentuk $a^n + 1$.

Bukti.

Berdasarkan persamaan (4) dengan memisalkan $\sqrt{R} = a+1$ dan $Q = a$,

$$V_n(a+1,a) = \left(\frac{a+1+\sqrt{(a+1)^2-4a}}{2}\right)^n + \left(\frac{a+1-\sqrt{(a+1)^2-4a}}{2}\right)^n$$

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

$$= a^n + 1. \qquad \square$$

Berdasarkan Teorema 4 dengan ketentuan $\{V_n(4,3)\}$ yang merupakan $V_n = 3^n + 1$ maka $V_{\frac{F_n-1}{2}} = 3^{\frac{F_n-1}{2}}$ sehingga Teorema 2 dapat direvisi. Sebelum Teorema 2 direvisi diperlukan persamaan identitas berikut [4: h. 419]

$$V_{2n} = U_n V_n. \tag{8}$$

Berikut merupakan pengamatan yang dibuat untuk Teorema 2 yang merupakan uji Pepin direvisi menjadi Teorema berikut.

Teorema 5 ***Uji Pepin*** [3, h. 358] Bilangan Fermat $F_n = 2^{2^n} + 1$ dimana $n \geq 1$ adalah bilangan prima jika dan hanya jika

$$F_n \mid V_{\frac{F_n-1}{2}}(4,3).$$

Bukti.

Misalkan $\sqrt{R} = 4$ dan $Q = 3$ maka $\Delta = R - 4Q = 16 - 12 = 4$. Misalkan $F_n = 2^{2^n} + 1$ bilangan prima sehingga menurut persamaan (5) $\varepsilon = \left(\frac{\Delta}{F_n}\right) = \left(\frac{4}{F_n}\right) = \left(\frac{2}{F_n}\right)\left(\frac{2}{F_n}\right) = 1$ dan $\sigma = \left(\frac{R}{F_n}\right) = \left(\frac{16}{F_n}\right) = \left(\frac{4}{F_n}\right)\left(\frac{4}{F_n}\right) = 1$. Selain itu, karena $n > 1$, maka dengan menggunakan hukum resiprositas Gauss diperoleh

$$\left(\frac{3}{F_n}\right)\left(\frac{F_n}{3}\right) = \left(\frac{3}{2^{2^n}+1}\right)\left(\frac{2^{2^n}+1}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{2^{2^n}+1-1}{2}} = (-1)^{2^{n-1}} = 1.$$

Untuk $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, diperoleh

$$\tau = \left(\frac{Q}{F_n}\right) = \left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) \equiv \left(2^{2^n}+1\right)^{\frac{3-1}{2}} \equiv -1 \pmod 3.$$

Karena $\sigma\varepsilon = 1$, maka dengan Lema 2, $F_n \mid U_{2^{2^n}}$. Kemudian karena $\tau \neq \sigma$, maka dengan Lema 5 menyatakan bahwa $F_n \nmid U_{2^{2^n-1}}$. Dengan demikian, RoA dari F_n di $\{U_n(4,3)\}$ adalah 2^{2^n} yaitu $F_n - 1$. Sebaliknya, dengan Lema 3 RoA dari F_n adalah $2^{2^n - r}$, untuk suatu bilangan bulat positif r dan $F_n | U_{2^{2^n-1}}$. Berdasarkan Lema 4, $F_n | V_{\frac{F_n-1}{2}}$. Sebaliknya, memisalkan $F_n | V_{\frac{F_n-1}{2}}$ maka dengan persamaan (8) $F_n | U_{F_n-1}$. Secara khusus, $F_n | U_{2^{2^n}}$. Berdasarkan Lema 3, $\omega(F_n)$ harus menjadi pembagi dari 2^{2^n}. Namun, berdasarkan Lema 1, $U_{2^{2^n}}$ relatif prima terhadap $U_{2^{2^n-1}}$ sehingga berdasarkan Lema 6 $\omega(F_n) = 2^{2^n} = F_n - 1$ dan F_n adalah bilangan prima.□

Selanjutnya merevisi Teorema 3 yang merupakan uji Lucas-Lehmer yang menunjukkan bahwa barisan angka 4, 14, 194, 37634, 1416317954, ... adalah barisan Lehmer sekawan $\{V_n(\sqrt{2}, -1)\}$ yang merupakan pangkat 2. Sebelumnya diperlukan persamaan identitas [3, h. 419] berikut:

$$V_{2n} = V_n^2 - 2Q^n. \tag{9}$$

Diketahui $\{V_n(\sqrt{2}, -1)\}$ sehingga $V_2 = 4$. Berdasarkan Teorema 3 $S_k = S_{k-1}^2 - 2$, dimana $S_1 = 4 = V_2$. Karena $Q = -1$, maka menurut persamaan (9) menjadi $S_k = V_{2^k}$ untuk $k \in \{1, 2, \ldots\}$. Oleh karena itu, pernyataan tersebut diberikan pada Uji Lucas-Lehmer yang menegaskan M_n membagi $(n-1)$st yaitu 4, 14, 194, 37634, 1416317954, ... maka M_n adalah faktor dari $V_{2^{n-1}}$ sehingga dapat dikatakan setara dengan $M_n | V_{\frac{M_n+1}{2}}$. Bagian tersebut mempunyai bentuk setara dengan Teorema 3 yang direvisi sebagai berikut:

Teorema 6 ***Uji Lucas-Lehmer*** [3, h. 359] Bilangan $M_n = 2^n - 1$, dimana $n > 2$ adalah bilangan prima jika dan hanya jika

$$M_n | V_{\frac{M_n+1}{2}}(\sqrt{2}, -1).$$

Bukti.

Ambil $R = 2$, $Q = -1$ dan $\Delta = 6$, selanjutnya $\epsilon = -1$, $\sigma = 1$ dan $\tau = -1$ maka buktinya mengikuti bukti yang disajikan pada Teorema 5.□

Dapat diambil kesimpulan bahwa Teorema 5 dan Teorema 6 yang merupakan uji Pepin dan uji Lucas-Lehmer mempunyai bentuk setara dalam penyajian syarat perlu dan cukup, baik untuk bilangan Fermat maupun bilangan Mersenne.

DAFTAR PUSTAKA

[1] Burton, D. M. 2005. *Elementary Number Theory Edisi ke 6.* McGraw-Hill, New York.

[2] Carmichael, R. D. 1913. Onthe numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Annal of Mathematics*. 15: 30–70.

[3] Jaroma, J. H. 2009. Equivalence of Pepin's and the Lucas-Lehmer Tests, *European Journal of Pure and Applied Mathematics*. 2 : 352-360.

[4] Lehmer, D. H. 1930. An extended theory of Lucas' functions, *Annal of Mathematics*. 31: 419–448.

[5] Lehmer, D. H. 1935. On Lucas' test for the primality of Mersenne's numbers, *Journal London Math. Soc*.10: 162–165.

[6] Lucas, É. 1878. Théorie des fonctions numériques simplement périodiques. *American Journal of Mathematics*. 1: 184–240, 289–321.

[7] Lucas, É. 1879. Question 453, *Nouv. Cor. Math.* 5: 137.

[8] Pepin, T. 1877. Sur la formule$2^{2^n}+1$. *Comptes Rendus Academie Sciences.* 85: 329–331.

[9] Proth, F. 1876. Énoncés de divers théorèmes sur les nombres. *Comptes Rendus Academie Sciences.* 83: 1288–1289.

[10] Proth, F. 1878. Mémoires présentés, *Comptes Rendus Academie Sciences.* 87 : 374.

[11] Ribenboim, P. 1996. *The New Book of Prime Number Records*. Springer-Verlag, New York.

[12] Rosen, K. H. 2000. *Elementary Number Theory*, 4th ed., Addison Wesley Longman, Reading.

[13] Rosen, M. 1988. A proof of the Lucas-Lehmer test, *American Mathematical Monthly.* 95: 855–856.

[14] Tattersall, J. J. 2005. *Elementary Number Theory in Nine Chapters*, 2nd ed., Cambridge Univ. Press, Cambridge.

[15] Willams, H. C. 1998. *Edouard Lucas and Primality Testing*. John Wiley & Sons, New York.