Conspectus materiae tomi XXXVI, fasciculi 3

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'echange — Address of the Editorial Board and of the exchange — Die Adresse der Schriftleitung und des Austausches — Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-01330-3 ISSN 0065-1036

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XXXVI (1980)

Lehmer's numbers

by

A. Rotkiewicz (Warsaw) and R. Wasén (Djursholm)

The nth Lehmer number $u_n^{(f)}(\beta,\bar\beta)$ with respect to the trinomial $f(z)=z^2-\sqrt{L}\,z+M$ (L and M are rational integers) with the roots β and $\bar\beta$ is defined by

$$u_n^{(f)}(\beta,\bar\beta)=\begin{cases}(\beta^n-\bar\beta^n)/(\beta-\bar\beta) & \text{if } 2\nmid n,\\ (\beta^n-\bar\beta^n)/(\beta-\bar\beta^2) & \text{if } 2\mid n.\end{cases}\tag{1}$$

We shall write, for brevity, u_n instead of $u_n^{(f)}(\beta,\bar\beta)$.

Since $u_0=0$, $u_1=1$, $u_{n+2}=Lu_{n+1}-Mu_n$ for $2\nmid n$ and $u_{n+2}=u_{n+1}-Mu_n$ for $2\mid n$, the numbers u_n are rational integers and form a recurring sequence, the so-called Lehmer sequence with respect to $f(z)$. The nth term in the associated recurring sequence is defined by

$$v_n=v_n^{(f)}(\beta,\bar\beta)=\begin{cases}(\beta^n+\bar\beta^n)/(\beta+\bar\beta) & \text{if } 2\nmid n,\\ \beta^n+\bar\beta^n & \text{if } 2\mid n.\end{cases}\tag{2}$$

Since $v_0=2$, $v_1=1$, $v_{n+2}=Lv_{n+1}-Mv_n$ for $2\mid n$ and $v_{n+2}=v_{n+1}-Mv_n$ for $2\nmid n$, these numbers are rational integers. We can assume without any essential loss of generality that $(L,M)=1$ and $L>0$ (cf. [5]). In the sequel any trinomial $f=x^2-\sqrt{L}\,x+M$ is supposed to be such that L and M are rational integers,

$$K=L-4M=K(f)\neq 0,\quad L>0,\quad M\neq 0,\quad (L,M)=1.$$

One of the most interesting applications of the sequences v_n concerns tests of primality. In this context we have found it convenient to introduce the following concepts:

Definition 1. n satisfies the *Lucas condition* for $f=z^2-\sqrt{L}\,z+M$ iff n is odd, $(n,KL)=1$, and $n\mid V_{[n-(KL|n)]/2}$.

From Professors J. Brillhart and S. Wagstaff we get the following information.

Let p be odd, $p > 2$. Write $p-1 = d\cdot 2^s$, where d is odd and s is a positive integer. Then p is called a *strong pseudoprime to base t* if either

(3) $t^d \equiv 1 \pmod{p}$, or

(4) $t^{d\cdot 2^r} \equiv -1 \pmod{p}$ for a certain non-negative $r < s$.

The concept of strong pseudoprime, useful in the investigation of primality is due to John Selfridge. Pomerance, Selfridge and Wagstaff, Jr. gave a list of all pseudoprimes (composite) to base 2 below $25\cdot 10^9$ (see [20]).

An odd n which satisfies the Lucas condition for $f(z) = z^2-(t+1)z+t$ is a strong pseudoprime to base t satisfying (4) with $r = s-1$.

DEFINITION 2. A sequence $\{s_i\}_0^\infty$ of integers is called an *s-sequence* iff $s_i = s_{i-1}^2-2$ for $i \geqslant 1$.

For any trinomial f with roots $\beta, \bar\beta$, and for any natural number h, if $S_0 = V_{2h}^{(f)}/(\beta\cdot\bar\beta)^h$, then the following generalization of a well-known relation (cf. [18]) results by induction:

$$(\beta\cdot\bar\beta)^{h\cdot 2^{n-2}} S_{n-2} = V_{h\cdot 2^{n-1}}^{(f)}; \quad n \geqslant 2. \tag{5}$$

Denote by M_p the pth Mersenne number $M_p = 2^p-1$, where p is an odd prime. A well-known theorem of Lucas and Lehmer (see [4], [6], [18]) runs as follows:

M_p is a prime iff $M_p \mid S_{p-2}$, where $S_0 = 4$ and $\{S_i\}_0^\infty$ is an s-sequence.

If $f(z) = z^2-\sqrt{2}\,z-1$ then

$$S_{n-2} = V_{2^{n-1}}, \quad n \geqslant 2 \quad \text{if} \quad S_0 = 4. \tag{6}$$

Suppose that $m = M_p$ satisfies the Lucas condition for $f = z^2-\sqrt{2}z-1$. We have $(KL\mid 2^p-1) = (3\mid 2^p-1) = -1$ and $m \mid V_{[m-(KL|m)]/2} = V_{2^{p-1}}$. Now, by (6), $m = M_p \mid S_{p-2}$ and so by the theorem of Lucas and Lehmer M_p is a prime. On the other hand, if M_p is a prime, then $M_p \mid S_{p-2}$ by the theorem of Lucas and Lehmer. By (6) this implies that

$$M_p \mid V_{2^{p-1}}. \tag{7}$$

Since $m = M_p$ is a prime, M_p is odd and $2 \mid M_p-(KL\mid M_p) = 2^p$ ($L = 2$, $(KL\mid M_p) = (3\mid M_p) = -1$), we have by (7) $m = M_p \mid V_{[m-(KL|m)]/2}$ and $m = M_p$ satisfies the Lucas condition for $f = z^2-\sqrt{2}z-1$. Hence the Lucas and Lehmer theorem can be given in the following equivalent form:

REFORMULATION OF THE LUCAS AND LEHMER THEOREM (a particular case of Theorem 1). *M_p is a prime iff M_p satisfies the Lucas condition for $f = z^2-\sqrt{2}\,z-1$.*

In a similar way we arrive at the following reformulation of theorems of Pepin and Proth:

PEPIN'S THEOREM. *The Fermat number $F_n = 2^{2^n}+1$ is a prime iff* $F_n \mid 3^{(F_n-1)/2}+1$ (see [1], p. 376).

PROTH'S THEOREM. *Let $N = k\cdot a^n+1$ where $0 < k < 2^n$. Suppose that $(a\mid N) = -1$. Then N is a prime iff $a^{(N-1)/2} \equiv -1 \pmod{N}$* (see [11], [12], [17]).

REFORMULATION OF PEPIN'S THEOREM (a particular case of Proth's theorem). *F_n is a prime iff F_n satisfies the Lucas condition for $f = z^2-4z+3$.*

REFORMULATION OF PROTH'S THEOREM (a particular case of the reformulation of Riesel's theorem). *Let N and a satisfy the conditions of Proth's theorem; then N is a prime iff N satisfies the Lucas condition for $f = z^2-(a+1)z+a$.*

The following theorem of Riesel can also be reformulated.

RIESEL'S THEOREM (see Theorem 5 in [10]). *Suppose that $n \geqslant 2$, h is odd $< 2^n$, $N = h\cdot 2^n-1$, $r = |a^2-b^2D|$ with square free D, $\beta = (a+b\sqrt{D})^2/r$ integer in $Q(\sqrt{D})$, $(\beta, N) = 1$ in $Q(\sqrt{D})$, $(D/N) = -1$ and $(r\mid N)(a^2-b^2D)/r = -1$. Then a necessary and sufficient condition that N be a prime is*

$$S_{n-2} \equiv 0 \pmod{N} \quad \text{if} \quad S_v = S_{v-1}^2-2 \quad \text{with} \quad S_0 = \beta^h+\beta^{-h}. \tag{8}$$

Note that β is a unit. Hence if β is not up to a sign a power of the fundamental unit in $Q(\sqrt{D})$, then β must be a root of unity. We have the following three possible cases: (I) $\beta = \pm 1$; (II) $\beta = \pm i$; (III) $\beta = \pm(-1\pm\sqrt{-3})/2$.

By a straightforward calculation it may be shown that (I) is impossible. This case corresponds to the situation where $ab = 0$. Hence without any loss of generality we may assume that $ab \neq 0$. Case (III) can likewise be shown to be impossible. Case (II) corresponds to the only possible imaginary field in the method of Riesel, namely to the Gaussian field $Q(i)$. In this case his method works for exactly $N = 3$ nad $N = 11$. As noted by Riesel, a and b may be supposed to be rational integers. This follows directly from the definition of $\beta = (a+b\sqrt{D})^2/|a^2-b^2D|$ since if a, b equal, respectively, $a'/2$ and $b'/2$, a' and b' being odd rational integers, then $\beta = (a'+b'\sqrt{D})^2/|a'^2-b'^2D|$. Moreover, a similar argument may be applied to show that we may also assume that $(a, b) = 1$ and that $a > 0$ and $b > 0$. Altogether this implies that a and b may always be assumed to be relatively prime natural numbers. In practice, Riesel finds suitable a and b by taking the fundamental unit ε in $Q(\sqrt{D})$, where D is chosen so that $(D\mid N) = -1$, and writes it in the form $\varepsilon = (a+b\sqrt{D})^2/|a^2-b^2D|$ if ε has such a representation. Obviously Riesel chooses r as $|a^2-b^2D|$ in order to get a positive S_0.

THEOREM 1 (Reformulation of Riesel's theorem). *Suppose a, b, D, h and n satisfy the conditions in Riesel's theorem. Then $N = h\cdot 2^n-1$ is a prime iff N satisfies the Lucas condition for $f = z^2-2az+(a^2-Db^2)$.*

First we shall prove the following

LEMMA 1. *If a, b, D, h and n satisfy the conditions in the Riesel theorem, $\{S_i\}_0^\infty$ denotes the s-sequence in the Riesel theorem and $\{S_i^*\}_0^\infty$ the s-sequence determined by*

$$S_0^* = [(a+b\sqrt{D})^{2h}+(a-b\sqrt{D})^{2h}]/(a^2-b^2D)^h,$$

then $S_0^* = S_0 \operatorname{sgn}(a^2-b^2D)$.

Proof. I. $a^2-b^2D>0$. We have

$$S_0^* = [(a+b\sqrt{D})^{2h}+(a-b\sqrt{D})^{2h}]/|a^2-b^2D|^h = \beta^h+\bar\beta^h = \beta^h+\beta^{-h} = S_0.$$

II. $a^2-b^2D<0$. We get

$$S_0^* = -(\beta^h+\beta^{-h}) = -S_0.$$

This completes the proof of Lemma 1.

Proof of Theorem 1. Suppose that a, b, D, h and n satisfy the conditions in the Riesel theorem and that $\{S_i\}_0^\infty$ and $\{S_i^*\}_0^\infty$ are as in Lemma 1. We note that $(\beta, N) = 1$ in $Q(\sqrt{D})$ implies that $(r, N) = 1$ in $Q(\sqrt{D})$. Now if N is a prime, then by the Riesel theorem

$$N\mid S_{n-2} \tag{9}$$

and so by Lemma 1

$$N\mid S_{n-2}^*. \tag{10}$$

If $f = z^2-2az+(a^2-b^2D)$ then, since

$$S_0^* = [(a+b\sqrt{D})^{2h}+(a-b\sqrt{D})^{2h}]/(a^2-b^2D)^h$$

if γ and $\bar\gamma$ denote the roots of f, we get

$$(\gamma\cdot\bar\gamma)^{h\cdot 2^{n-2}}\cdot S_{n-2}^* = V_{h\cdot 2^{n-1}}^{(f)};\quad n\geqslant 2 \tag{11}$$

and, by (10), $N\mid V_{h\cdot 2^{n-1}}^{(f)}$. Now $D(f) = 4b^2D$ so $(D(f)\mid N) = (4b^2D\mid N) = -1$. Hence $[N-(D(f)\mid N)]/2 = h\cdot 2^{n-1}$ and so $N\mid V_{h\cdot 2^{n-1}}^{(f)}$ implies that N satisfies the Lucas condition for f. On the other hand, if N satisfies the Lucas condition for f, then $N\mid V_{h\cdot 2^{n-1}}^{(f)}$ and so by (11), $N\mid (\gamma\cdot\bar\gamma)^{h\cdot 2^{n-2}}\times\times S_{n-2}^*$. But $\gamma\cdot\bar\gamma = \pm r = \pm|a^2-b^2D|$ and $(r, N) = 1$ in $Q(\sqrt{D})$ and so certainly also in Q and we have $N\mid S_{n-2}^* = \pm S_{n-2}$. This completes the proof of Theorem 1.

In view of what we have already shown it would be of interest to know if there are infinitely many composite numbers satisfying the Lucas condition for any fixed trinomial f. For a special class of composite numbers satisfying the Lucas condition, namely those corresponding to trinomials with positive discriminant, we prove the following stronger

THEOREM 2. *Let $K = K(f)>0$. Every arithmetical progression $ax+b$, where $(a, b) = 1$, which contains prime numbers n such that*

$$n\mid V_{[n-(KL|n)]/2}^{(f)},\qquad (n, 2KL) = 1 \tag{12}$$

contains also composite numbers n which satisfy (12), i.e. every arithmetical progression $ax+b$, where $(a, b) = 1$, which contains prime numbers which satisfy the Lucas condition contains also infinitely many composite numbers n satisfying the Lucas condition for any fixed trinomial $f = z^2-\sqrt{L}z+M$.

We shall write, for brevity, K instead $K(f)$ and V instead of $V^{(f)}(\beta, \bar\beta)$.

The idea of the proof of Theorem 2 consists in using the conditions in the theorem to show that if the prime p and the number k satisfy certain conditions in which k is chosen as a suitable function of p, then $p\in\{ax+b\}$, $k\in\{ax+1\}$, $k>1$, $(p, k) = 1$, $p\mid V_{[kp-(KL|kp)]/2}$ and $k\mid V_{[kp-(KL|kp)]/2}$ and so of course $pk\in\{ax+b\}$ and pk is a composite number satisfying the Lucas condition for f. Then we show that there are infinitely many couples $\langle p, k\rangle$ satisfying these conditions, and so the proof is complete.

With no essential loss of generality we can assume that $2\mid a$ and $2\nmid b$.

We write $c = m(ML)$ for the conductor of the quadratic character $(ML|n)$ and denote by R_{ML} and $\bar R_{ML}$ the sets of residues $\bmod m(ML)$ for which this character takes the values $+1$ and -1, respectively. Then the following facts are well known:

$$|R_{ML}| = |\bar R_{ML}| = \tfrac{1}{2}\varphi(m(ML)); \tag{13}$$

(14) For any proper divisor d of $m(ML)$, for any g, where $(g, d) = 1$ there is at least one element in R_{ML} and $\bar R_{ML}$ congruent to $g \bmod d$;

(15) $m(ML)\mid 4\cdot ML$ and if $m(ML)\equiv 0 \pmod 2$ then $4\mid m(ML)$.

LEMMA 2. *For all pairs of arithmetical progressions $\{a_1x+b_1\}$, $\{a_2x+b_2\}$ such that $(a_1, b_1) = 1$, $(a_2, b_2) = 1$, if $\{a_1x+b_1\}\cap\{a_2x+b_2\}\neq\emptyset$ then there are a_3, b_3 such that $\{a_1x+b_1\}\cap\{a_2x+b_2\} = \{a_3x+b_3\}$, where $(a_3, b_3) = 1$.*

The proof may be omitted.

LEMMA 3. *Let $K = K(f)>0$, $(L, M) = 1$, $(a, b) = 1$, $2\mid a$, $c = m(ML)\nmid a$ or $c\mid a$ and $b\equiv d_i \pmod c$ for a certain $d_i\in\bar R_{ML}$; then there exist infinitely many s which satisfy the following relations:*

$$(as+b, KL) = 1,\qquad as+b>1, \tag{16}$$

$$as+b\equiv d_i \pmod c\quad \text{for some } d_i\in\bar R_{ML}. \tag{17}$$

Proof. I. $c \nmid a$. In this case $d = (a, c) \geqslant 1$ is a proper divisor of c and $(d, b) = 1$. Hence (14) applies and ensures that there is a $d_i \in \bar{R}_{ML}$, $(d_i, c) = 1$ such that

(18) $$d \mid d_i - b, \quad (d_i, c) = 1.$$

We regroup (17) and get

(19) $$a \cdot s \equiv d_i - b \pmod c \quad \text{with} \quad c = m(ML).$$

On putting $a/d = a'$, $c/d = c'$ we get

(20) $$a's \equiv \frac{d_i - b}{d} \pmod{c'}.$$

Since $(a', c') = 1$ and $d \mid d_i - b$, (20) is solvable and all solutions are given by $\{c'x + r\}$, $x = 0, 1, 2, \ldots$ for a suitable r. Since $s = c'x + r$, we have $as + b = a(c'x + r) + b = ac'x + (ra + b)$. If $(ac', ar + b) > 1$, then there exists an odd prime p such that $p \mid c'$, $p \mid ra + b$. Then $p \mid as + b = ac'x + (ra + b)$, $p \mid c$. But $as + b \equiv d_i \pmod c$, and hence $p \mid d_i$, which is impossible, since $(c, d_i) = 1$. By Dirichlet's theorem there are infinitely many x such that $as + b = ac'x + (ra + b)$ is a prime $> KL$. Then (16) and (17) hold.

II. $c \mid a$. In this case it is obviously necessary and sufficient that $b \equiv d_i \pmod c$ for a certain d_i in $\bar{R}_{ML}$ in order that (17) be satisfied. If $c \mid a$, $b \equiv d_i \pmod c$, then for every s: $as + b \equiv d_i \pmod c$. If $as + b$ is a prime $> KL$, then (16) and (17) hold. This completes the proof of Lemma 3.

Now we shall give well-known facts from the theory of Lehmer's numbers.

Put

$$Q_n = Q_n^{(f)}(\beta, \bar{\beta}) = \prod_{\substack{r=1 \\ (r,n)=1}}^{n} (\beta - \zeta_n^r \bar{\beta}) = \prod_{i \mid n} (\beta^i - \bar{\beta}^i)^{\mu(n/i)},$$

where ζ_n is a primitive nth root of unity and μ is the Möbius function.

We have

$Q_n \mid u_n$; $Q_n \mid V_{n/2}$ if $2 \mid n$; $V_m \mid V_n$ iff $2 \nmid \frac{n}{m}$, $m \mid n$; $p \mid u_{p-(KL|p)}$, if p is an odd prime and $(KL, p) = 1$.

$u_m \mid u_n$ if $m \mid n$; $p \mid V_{[p-(KL|p)]/2}$ if p is an odd prime, $(KL, p) = 1$ and $(ML \mid p) = -1$.

Let $\{cx + d_i\}$, $i = 1, 2, \ldots, \varphi(c)/2$ be the $[\varphi(c)]/2$ arithmetical progressions with minimal difference determining the odd primes for which ML is a quadratic non-residue, $\{d_i\}_{i=1}^{\varphi(c)/2} = \bar{R}_{ML}$.

We denote by $\Psi(p)$ the assertion that for an odd prime p there exist integers s, d_i and λ satisfying the following conditions:

(21) $p \equiv b \pmod a$, $(KL, p) = 1$, $(ML \mid p) = -1$;

(22) $p - (KL \mid p) = 2^\lambda p_1 p_2 p_3 q^2 h$, where p_1, p_2, p_3 and q are odd primes, $(2p_1p_2p_3q, h) = 1$;

(23) $2^\lambda \| as + b - (KL \mid as + b)$, $(2^\lambda aKL, c) \mid sa + b - d_i$;

(24) $as + b > 1$, $(KL, as + b) = 1$, $d_i \in \bar{R}_{ML}$,

(25) $(acKL, p_1p_2p_3) = 1$,

(26) $2^\lambda acKLp_1p_2p_3\varphi_1(2^\lambda acKLp_1p_2p_3) \mid q - 1$, *where* $\varphi_1(q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_\varrho^{\lambda_\varrho}) = 2q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_\varrho^{\lambda_\varrho}(q_1^2 - 1)(q_2^2 - 1) \ldots (q_\varrho^2 - 1)$.

LEMMA 4. *If $K > 0$ then $Q_n > 0$.*

Proof. Since Q_n is symmetrical in β and $\bar{\beta}$, we may assume that $\beta = (\sqrt{L} + \sqrt{K})/2 \geqslant 1$; hence $\beta^i - \bar{\beta}^i > 0$ and the lemma follows from the formula $Q_n = \prod_{i \mid n} (\beta^i - \bar{\beta}^i)^{\mu(n/i)}$.

LEMMA 5. *If $q^2 \| n$, $m\varphi_1(m) \mid q - 1$ where q is a prime, then*

$$Q_n \equiv 1 \pmod m.$$

For the proof see Lemma 5 of [13].

A prime p is called a *primitive prime factor of the number* u_n if $p \mid u_n$ but $p \nmid KLu_3 \ldots u_{n-1}$. It is a well-known fact (see [16]) that if $K > 0$, $n > 12$ then u_n has at least one primitive prime factor and all primitive prime factors of u_n are divisors of Q_n. Hence if $n_1, n_2 > 12$, $K > 0$ then $Q_{n_1} = Q_{n_2}$ implies $n_1 = n_2$. This means that for $n > 12$, $K > 0$ we may introduce the notion $J(k) = n$ if $k = Q_n$.

LEMMA 6. *Let $n \neq 2^v$, $3 \cdot 2^v$; then*

I. *The greatest prime divisor r of n divides Q_n iff r is a primitive prime factor of u_{n/r^ω}, where $r^\omega \| n$;*

II. *All prime factors u of Q_n different from r are primitive factors of u_n, they are relatively prime to KL and they are of the form $nx + (KL \mid u)$.*

For the proof of Lemma 6 see [5].

COROLLARY. *(22) and (26) imply that for at least one $i \leqslant 3$ we have*

(27) $$p \mid Q_{[p-(KL|p)]/p_i},$$

(28) *the greatest prime factor of $[p - (KL \mid p)]/p_i$ does not divide $Q_{[p-(KL|p)]/p_i}$.*

Proof. Put $k_i = Q_{[p-(KL|p)]/p_i}$, $i = 1, 2, 3$. Suppose that $p \mid k_i$ for at least two i's. Since $[p - (KL \mid p)]/p_i \neq 2^v, 3 \cdot 2^v$, $i = 1, 2, 3$, Lemma 6 implies and ensures, in view of $p > [p - (KL \mid p)]/p_i$, $i = 1, 2, 3$, that p is a primitive prime factor of the numbers $u_{J(k_i)}$ $(J(k_i) > 12)$, which is impossible since $i \neq j$ implies that $J(k_i) \neq J(k_j)$. Hence we may assume that $p \nmid k_1$ and $p \nmid k_2$. Denote by r the greatest prime divisor of $p-(KL|p)$. Since $r \geqslant q > p_1p_2p_3$, in view of $q^2|p-(KL|p), p_1p_2p_3|q-1$ we have $r > p_1$ and $r > p_2$ and so r is the greatest prime factor of $J(k_1)$ and $J(k_2)$. Hence in order to complete the proof it is enough to show that $r \nmid k_1$ or $r \nmid k_2$. If $r|k_1$ and $r|k_2$, then by Lemma 6 I it follows that r is a primitive factor of $u_{J(k_1)/r^\omega}$ and $u_{J(k_2)/r^\omega}$, where $r^\omega \| [p-(KL|p)]/p_i$; $i = 1, 2, 3$, which is impossible since certainly $J(k_1)/r^\omega \neq J(k_2)/r^\omega$.

By $\Psi(p, k)$ we denote the conjunction of $\Psi(p)$, (27), (28) and the equality

$$k = Q_{[p-(KL|p)]/p_i}. \tag{29}$$

Lemma 7. *$\Psi(p, k)$ implies that*

(a) $k \equiv 1 (\bmod 2^\lambda acKLp_1p_2p_3)$,

(b) $(k, KL) = 1$, $(KL|k) = 1$,

(c) *every prime divisor q_i of k is prime to KL and* $\equiv (KL|q_i) \big(\bmod J(k)\big)$,

(d) $k \equiv (KL|k) \big(\bmod J(k)\big)$,

(e) $k \equiv 1 \big(\bmod 2[p-(KL|p)]\big)$,

(f) $[p-(KL|p)]/2 \,|\, [kp-(KL|kp)]/2$; $\{[kp-(KL|kp)]/[p-(KL|p)]\} \equiv 1 (\bmod 2)$,

(g) $k \,|\, V_{[p-(KL|p)]/2}$,

(i) $p \,|\, V_{[pk-(KL|pk)]/2}$,

(j) $k \,|\, V_{[pk-(KL|pk)]/2}$,

(k) *pk is a composite number satisfying the Lucas condition and is of the form $ax+b$.*

Lemma 8. *If s, d_i, λ are integers and q, p_1, p_2, p_3 are distinct odd primes satisfying the relations* (23)–(26) *then there exists an integer m such that*

$$m \equiv b+sa (\bmod 2^\lambda aKL),$$

$$m \equiv d_i (\bmod c), \quad c = m(ML), \tag{30}$$

$$m \equiv (KL|b+sa)+lq^2 (\bmod l^2q^3), \quad \textit{where} \quad l = p_1p_2p_3,$$

and all primes p in the progression

$$2^\lambda acKLl^2q^3x+m, \tag{31}$$

satisfy $\Psi(p)$, the above progression represents infinitely many primes and for each of them there exists a $k \equiv 1 (\bmod a)$ such that pk is a composite number satisfying the Lucas condition for $f = z^2-\sqrt{L}z+M$, $\equiv b (\bmod a)$.

Proof of Lemma 7. Since $2^\lambda acKLp_1p_2p_3\varphi_1(2^\lambda acKLp_1p_2p_3)|q-1$, $q^2 \| [p-(KL|p)]/p_i$, Lemma 5 applies and we get $k = Q_{[p-(KL|p)]/p_i}$ $\equiv 1 (\bmod 2^\lambda acKLp_1p_2p_3)$ and (a) holds.

Now $2|a$ and so, by (a), $k \equiv 1 (\bmod 4KL)$, and thus certainly $(KL, k) = 1$; hence $(KL|k) = (KL|4KLx+1) = (KL|1) = 1$.

Since $p-(KL|p) = 2^\lambda p_1p_2p_3q^2h$, we have $[p-(KL|p)]/p_i \neq 2^v$, $3\cdot 2^v$. By Lemma 6 II, (c) now follows directly.

Say that $k = \prod_{i=1}^{h} q_i^{\lambda_i}$ is the decomposition of k into prime factors. By (b), $(KL|k) = 1$. We have by (c),

$$k = \prod_{i=1}^{h} q_i^{\lambda_i} \equiv \prod_{i=1}^{h} (KL|q_i)^{\lambda_i} \equiv (KL|k) \big(\bmod J(k)\big)$$

and (d) holds.

By (b) and (d) we have $k \equiv 1 \big(\bmod [p-(KL|p)]/p_i\big)$, where $[p-(KL|p)]/p_i = J(k)$. Now, by (a), $k \equiv 1 (\bmod p_i)$. Since $p_i \| p-(KL|p)$ and $2^\lambda \| p-(KL|p)$, we have: $k \equiv 1 \big(\bmod 2[p-(KL|p)]\big)$ and the proof of (e) is complete.

Since $(KL, p) = 1$ and $(KL|k) = 1$ by (b), from (e) it follows that

$$kp-(KL|kp) = \big[2\big(p-(KL|p)\big)t+1\big]p-(KL|k)(KL|p)$$

or a certain t. Since, by (b), $(KL|k) = 1$, we have

$$[kp-(KL|kp)]/2 = (2pt+1)[p-(KL|p)]/2$$

and this completes the proof of (f).

Formula (g) follows directly from the formula $Q_n | V_{n/2}$, where $2|n$.

From (f) it follows that $V_{[p-(KL|p)]/2} \,|\, V_{[pk-(KL|pk)]/2}$ and, since $(LM|p) = -1$, we have: $p \,|\, V_{[p-(KL|p)]/2}$ and (i) follows. Since by (g), $k \,|\, V_{[p-(KL|p)/2]}$, thus $k \,|\, V_{[p-(KL|p)]/2} \,|\, V_{[pk-(KL|pk)]/2}$ and (j) holds.

Since $p \equiv b (\bmod a)$, $k \equiv 1 (\bmod a)$, $(p, k) = 1$, (k) follows from (i) and (j).

Proof of Lemma 8. The linear system of congruences $x \equiv b_1 (\bmod m_1)$, $x \equiv b_2 (\bmod m_2)$ is solvable iff $(m_1, m_2)|b_1-b_2$ and the solutions belong to $\left\{\frac{m_1m_2}{(m_1, m_2)}x+em_1+b_1\right\}$, where e is a solution of the congruence $\frac{m_1}{(m_1, m_2)}x \equiv \frac{b_2-b_1}{(m_1, m_2)} \left(\bmod \frac{m_2}{(m_1, m_2)}\right)$. The question of the solvability of the linear congruences $x \equiv b_1 (\bmod m_1)$, $x \equiv b_2 (\bmod m_2)$ is equivalent to the question whether $\{m_1x+b_1\} \cap \{m_2x+b_2\} = \left\{\frac{m_1m_2}{(m_1, m_2)}x+em_1+b_1\right\}$ for a certain e.

In our case, since $(2^\lambda aKL, c)|b+sa-d_i$, the congruence system $x \equiv b+sa (\bmod 2^\lambda aKL)$, $x \equiv d_i (\bmod c)$ is solvable and exactly all solutions belong to $\left\{\frac{2^\lambda aKLc}{(2^\lambda aKL,c)}x+e\cdot 2^\lambda aKL+b+sa\right\}$ for a certain e. Since $(2^\lambda aKLc,\ p_1p_2p_3)=1$, $(2^\lambda acKL,q)=1$, $l=p_1p_2p_3$ it follows that $(2^\lambda aKLc, l^2q^3)=1$. Thus

$$\left\{\frac{2^\lambda aKLc}{(2^\lambda aKL,c)}x+e\cdot 2^\lambda aKL+b+sa\right\}\cap\{l^2q^3x+(KL|b+sa)+l\cdot q^2\}\neq\emptyset$$

and this implies that any number m in this intersection satisfies the linear system $m\equiv b+sa(\mathrm{mod}\ 2^\lambda aKL)$, $m\equiv d_i(\mathrm{mod}\ c)$, $m\equiv(KL|b+sa)+ +l^2(\mathrm{mod}\ l^2q^3)$. Next we prove that if m is a number satisfying the last linear system, then $\Psi(p)$ holds for all primes p in the progression $2^\lambda acKLl^2q^3x+m$.

Since $m\equiv b(\mathrm{mod}\ a)$ and all the primes in the progression $2^\lambda acKLl^2q^3x+ +m$ are $\equiv m(\mathrm{mod}\ a)$, we have $p\equiv b(\mathrm{mod}\ a)$. Moreover, $(KL,p)>1$ implies in view of $m\equiv b+sa(\mathrm{mod}\ 2^\lambda aKL)$ that $(KL,b+sa)>1$, which is impossible in view of the assumption of our lemma, and hence the condition $(KL,p)=1$ is satisfied. Since $m\equiv d_i(\mathrm{mod}\ c)$, we have $(ML|p)=-1$. Since $2\nmid b+sa>1$, $\lambda\geqslant 1$, $2|a$, we have $p\equiv b+sa(\mathrm{mod}\ 4KL)$, $p=b+ +sa+4KLx$. In view of the fact that $2\nmid b+sa$ for all s we get $(KL|b+sa)=(KL|b+sa+4KLx)=(KL|p)$.

Since $p\equiv m(\mathrm{mod}\ l^2q^3)$ and $m\equiv(KL|b+sa)+p_1p_2p_3q^2(\mathrm{mod}\ p_1^2p_2^2p_3^2q^3)$, it follows that $p-(KL|p)\equiv lq^2(\mathrm{mod}\ l^2q^3)$ and so we have $p_i\|p-(KL|p)$ for $i=1,2,3$ and $q^2\|p-(KL|p)$. Since p belongs to the progression $2^\lambda acKLl^2q^3x+m$, we have $p=2^\lambda aKLcs_1+m$ for a certain s_1. Since $m=b+sa+2^\lambda aKLs_2$, we get

$$p-(KL|p)=2^\lambda aKLcs_1+2^\lambda aKLs_2+\big(b+sa-(KL|b+sa)\big)$$

in view of $(KL|p)=(KL|b+sa)$.

Since by (23), $2^\lambda\|b+sa-(KL|b+sa)$, we have in view of $2|a$, $2^\lambda\|p-(KL|p)$.

If $(p,l)>1$ then, since $p\equiv m(\mathrm{mod}\ l)$ by (31), by (30) we get $|(KL|b+sa)|>1$, which is absurd.

Finally we prove that the progression $2^\lambda acKLl^2q^3x+m$ represents infinitely many primes. In view of Dirichlet's theorem on primes in arithmetical progression it is clearly enough to show that $(2^\lambda acKLl^2q^3,m)=1$.

Since b is odd and $2|a$ by (30), it follows that $2\nmid m$ and so $(m,2^\lambda)=1$. $(m,a)=1$ since otherwise, by (30), $(a,b+sa)>1$ in contradiction to the condition in the lemma that $(a,b)=1$. $(m,c)=1$ since otherwise, by (30), $(d_i,c)>1$, which is impossible since $cx+d_i$ represents infinitely many primes, $(KL,m)=1$ since otherwise $(KL,b+sa)>1$ by (30) in contradiction to (24); hence in order to complete the proof it is enough to show that $(lq,m)=1$, and this is clear in view of (30).

Hence there are infinitely many primes p satisfying $\Psi(p)$. Moreover, by Corollary to Lemma 6 for each such prime p there is a k such that

$k=Q_{[p-(KL|p)]/p_i}$ satisfies (27) and (28). Hence we have $\Psi(p,k)$ and so, by Lemma 7, pk is a composite number satisfying the Lucas condition for $f=z^2-\sqrt{L}z+M$ and belonging to $ax+b$. This completes the proof of Lemma 8.

LEMMA 9. *Any arithmetical progression $ax+b$ such that $(a,b)=1$ and $c=m(ML)\nmid a$ contains infinitely many composite numbers satisfying the Lucas condition for any fixed trinomial $f=z^2-\sqrt{L}z+M$, where $K(f)>0$.*

If $c=m(ML)|a$, $K=K(f)>0$, then $ax+b$ contains infinitely many composite numbers satisfying the Lucas condition for f if $b\equiv d_i(\mathrm{mod}\ c)$ for a certain $d_i\in\bar{R}_{ML}$.

Proof of Lemma 9. We may find three distinct odd primes p_1,p_2 and p_3 such that $(acKL,l)=1$, where $l=p_1p_2p_3$. This follows in fact from the existence of infinitely many primes. Choose for example the three smallest such primes. By Lemma 3 there exist infinitely many s which satisfy the following relations:

$$(as+b,KL)=1,\qquad as+b\equiv d_i(\mathrm{mod}\ c)$$

for some $d_i\in\bar{R}_{ML}$. We define λ by the condition $2^\lambda\|b+sa-(KL|b+sa)$. Clearly $(2^\lambda aKL,c)|b+sa-d_i$. Next by Dirichlet's theorem there are infinitely many primes q such that $2^\lambda acKLl\varphi_1(2^\lambda acKLl)|q-1$. Take for example the smallest such q. By Lemma 8 there is an m which satisfies (30). Now Lemma 9 follows from Lemma 8.

Proof of Theorem 2. If the arithmetical progression $ax+b$, where $(a,b)=1$ contains prime numbers p such that $p|V_{[p-(KL|p)]/2}$, $(p,2KL)=1$, where $K>0$, then $(ML|p)=-1$ and $p\in\{cx+d_i\}$ for a certain $d_i\in\bar{R}_{ML}$ and $\{ax+b\}\cap\{cx+d_i\}\neq\emptyset$. By Lemma 2: $\{ax+b\}\cap \cap\{cx+d_i\}=\{a_3x+b_3\}$, where $(a_3,b_3)=1$. Then $c\nmid a$ or in the case $c|a$ there exists such a $d_i\in\bar{R}_{ML}$ that $b\equiv d_i(\mathrm{mod}\ c)$ for a certain $d_i\in\bar{R}_{ML}$, $(d_i,c)=1$. Now Theorem 2 follows from Lemma 9.

COROLLARY 1. *In every arithmetical progression $ax+b$ such that $(a,b)=1$ and $12\nmid a$ or $12|a$ and $b\equiv\pm 5(\mathrm{mod}\ 12)$ there are infinitely many composite numbers satisfying the Lucas condition for any fixed trinomial $z^2-Lz+3M^2=f(z)$, where $K(f)>0$.*

Remark. The Lucas numbers with respect to the polynomial $z^2- -Lz+M$ correspond to the Lehmer numbers with respect to the polynomial

$$z^2-\sqrt{\frac{L^2}{(L^2,M)}}z+\frac{M}{(L^2,M)}=z^2-\sqrt{L_1}z+M_1;\ K=L^2-4M,\ K_1=L_1-4M_1.$$

We have

$$(L_1M_1|p)=\left(\frac{L^2}{(L^2,M)}\cdot\frac{M}{(L^2,M)}\,\Big|\,p\right)=(M|p)\quad\text{for}\quad(LM,p)=1$$

and

$$(K_1L_1|p) = ((L_1-4M_1)L_1|p) = \left(\left(\frac{L^2}{(L^2,M)} - \frac{4M}{(L^2,M)}\right)\frac{L^2}{(L^2,M)}\middle|p\right)$$
$$= (L^2-4M|p) = (K|p) \quad \text{for} \quad (KL,p) = 1.$$

In the case of the Lehmer numbers with respect to the polynomial $z^2-\sqrt{L}z+M$ we can assume without loss of generality that $(L, M) = 1$. (This is not true for the Lucas numbers.) This follows from the equality

$$(\sqrt{dL_1}+\sqrt{dL_1-4M_1d})^n \pm (\sqrt{dL_1}-\sqrt{dL_1-4M_1d})^n$$
$$= (\sqrt{d})^n[(\sqrt{L_1}+\sqrt{L_1-4M_1})^n \pm (\sqrt{L_1}-\sqrt{L_1-4M_1})^n],$$

where $d = (L, M)$, $L = L_1d$, $M = M_1d$.

Proof of Corollary 1. The Lucas numbers with respect to the polynomial $z^2-Lz+3M^2$ correspond to the Lehmer numbers with respect to the polynomial $z^2-\sqrt{L^2/(L^2,3M^2)}z+3M^2/(L^2,3M^2)$. We have

$$m\left(\frac{L^2}{(L^2,3M^2)}\cdot\frac{3M^2}{(L^2,3M^2)}\right) = m(3M^2) = m(3) = 12, \quad \bar{R}_3 = \{5, 7\}$$

and Corollary 1 follows directly from Lemma 9. For example there exist infinitely many composite numbers satisfying the Lucas condition in the arithmetic progression $ax+b$ (where $(a, b) = 1$, $12\nmid a$ or $12|a$ and $b \equiv \pm 5 \pmod{12}$) for the polynomial z^2-4z+3 and so there are infinitely many odd composite n in $ax+b$ such that $n|3^{(n-1)/2}+1$ (cf. [15]).

Corollary 2. *In every arithmetic progression $ax+b$ such that $(a, b) = 1$ and $8\nmid a$ or $8|a$ and $b \equiv 5, 7 \pmod 8$ there are infinitely many composite numbers satisfying the Lucas condition for any fixed trinomial $z^2-Lz-2M^2 = f(z)$ where $K(f) > 0$.*

Proof. The Lucas numbers with respect to the polynomial $z^2-Lz-2M^2$ correspond to the Lehmer numbers with respect to the polynomial $z^2-\sqrt{L^2/(L^2,2M^2)}z-2M^2/(L^2,2M^2)$. We have

$$m\left(\frac{L^2}{(L^2,2M^2)}\cdot\frac{-2M^2}{(L^2,2M^2)}\right) = m(-2) = 8, \quad \bar{R}_{-2} = \{5, 7\}$$

and Corollary 2 follows directly from Lemma 9.

For example the Lucas numbers with respect to the polynomial z^2-2z-2 correspond to the Lehmer numbers with respect to the polynomial $z^2-\sqrt{2}z-1$ (here $K = 6$, $L = 2$) and there are infinitely many odd composite n coprime with 12 in $ax+b$, where $(a, b) = 1$, and $8\nmid a$ or $8|a$ and $b \equiv \pm 3 \pmod 8$ such that

$$n|(1+\sqrt{3})^{(n+1)/2}+(1-\sqrt{3})^{(n+1)/2} \quad \text{if} \quad n \equiv 5, 7 \pmod{12},$$
$$n|(1+\sqrt{3})^{(n-1)/2}+(1-\sqrt{3})^{(n-1)/2} \quad \text{if} \quad n \equiv \pm 1 \pmod{12}.$$

This holds in view of the fact that $(KL|n) = (6\cdot 2|n) = (3|n) = -1$ if $n \equiv \pm 5 \pmod{12}$ and $(3|n) = 1$ if $n \equiv \pm 1 \pmod{12}$.

Corollary 3. *In every arithmetic progression $ax+b$ such that $(a, b) = 1$ and $4\nmid a$ or $4|a$ and $b \equiv 3 \pmod 4$ there are infinitely many composite numbers satisfying the Lucas condition for any fixed trinomial $z^2-Lz-M^2 = f(z)$, where $K(f) > 0$.*

Proof. The Lucas numbers with respect to the polynomial z^2-Lz-M^2 correspond to the Lehmer numbers with respect to the polynomial $z^2-\sqrt{L^2/(L^2,M^2)}z-M^2/(L^2,M^2)$. We have:

$$m\left(\frac{L^2}{(L^2,M^2)}\cdot\frac{-M^2}{(L^2,M^2)}\right) = m(-1) = 4, \quad \bar{R}_{-1} = \{3\}$$

and the corollary follows directly from Lemma 9.

For example, in every arithmetic progression $ax+b$ such that $(a, b) = 1$ and $4\nmid a$ or $4|a$ and $b \equiv 3 \pmod 4$ there are infinitely many composite numbers satisfying the Lucas condition for the trinomial $f = z^2-z-1$ and so there are infinitely many composite n in $ax+b$, coprime with 10 such that

$$n\left|\left(\frac{1+\sqrt{5}}{2}\right)^{(n-1)/2}+\left(\frac{1-\sqrt{5}}{2}\right)^{(n-1)/2}\right. \quad \text{if} \quad n \equiv \pm 1 \pmod 5$$

and

$$n\left|\left(\frac{1+\sqrt{5}}{2}\right)^{(n+1)/2}+\left(\frac{1-\sqrt{5}}{2}\right)^{(n+1)/2}\right. \quad \text{if} \quad n \equiv \pm 2 \pmod 5.$$

This holds in view of the fact that $K(z^2-z-1) = 5$, $(5|n) = 1$ if $n \equiv \pm 1 \pmod 5$ and $(5|n) = -1$ if $n \equiv \pm 2 \pmod 5$.

Corollary 4. *In every arithmetic progression $ax+b$ such that $(a, b) = 1$ and $8\nmid a$ or $8|a$, $b \equiv \pm 3 \pmod 8$ there are infinitely many composite numbers satisfying the Lucas condition for any fixed trinomial $z^2-Lz+2M^2 = f(z)$, where $K(f) > 0$.*

Proof. The Lucas numbers with respect to the polynomial $z^2-Lz+ +2M^2$ correspond to the Lehmer number with respect to the polynomial

$$z^2-\sqrt{L^2/(L^2,2M^2)}\,z+2M^2/(L^2,2M^2).$$

We have

$$m\left(\frac{L^2}{(L^2,2M^2)}\cdot\frac{2M^2}{(L^2,2M^2)}\right)=m(2)=8,\qquad \bar{R}_2=\{3,5\}$$

and Corollary 4 follows directly from Lemma 9. For example in every arithmetic progression $ax+b$ such that $(a,b)=1$ and $8\nmid a$ or $8\mid a$ and $b\equiv\pm 3 \pmod 8$ there are infinitely many composite numbers satisfying the Lucas condition for z^2-3z+2 and so in $ax+b$ there are infinitely many composite n such that $n\mid 2^{(n-1)/2}+1$.

References

[1] L. E. Dickson, *History of the theory of numbers*, 3 vols, New York 1952.

[2] H. J. A. Duparc, *On almost primes of the second order*, Report Z. W. Math. Center, Amsterdam, 1955-013, pp. 1–13.

[3] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford 1954.

[4] M. Kraitchik, *Théorie des nombres II*, Paris 1926.

[5] D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. 31 (1930), pp. 419–448.

[6] — *On Lucas's test for the primality of Mersenne's numbers*, J. London Math. Soc. 10 (1935), pp. 162–165.

[7] E. Lieuwens, *Fermat pseudoprimes*, Doctoral thesis, Delft 1971.

[8] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. 1 (1878), pp. 184–249, 289–321.

[9] H. Riesel, *A note on the prime numbers of the forms $N=(6a+1)2^{n-1}-1$ and $M=(6a-1)2^{2n}-1$*, Ark. Mat. 3 (1956), pp. 245–253.

[10] — *Lucasian criteria for the primality of $N=h\cdot 2^n-1$*, Math. of Computation 23 (1969), pp. 869–875.

[11] R. M. Robinson, *The converse of Fermat's theorem*, Amer. Math. Monthly 64 (1957), pp. 703–710.

[12] — *A report on primes of the form $k\cdot 2^n+1$ and on factors of Fermat numbers*, Proc. Amer. Math. Soc. 9 (1958), pp. 673–681.

[13] A. Rotkiewicz, *On the pseudoprimes of the form $ax+b$ with respect to the sequence of Lehmer*, Bull. Acad. Pol. Sci. Sér. Sci. Math. Astronom. Phys. 20 (1972), pp. 349–354.

[14] — *On the pseudoprimes with respect to the Lucas sequences*, ibid. 21 (1973), pp. 793–797.

[15] — *Remarque sur un théorème de F. Proth*, Mat. Vesnik 1 (16) (1964), pp. 244–245.

[16] A. Schinzel, *On primitive factors of Lehmer numbers I*, Acta Arith. 8 (1963), pp. 213–223.

[17] W. Sierpiński, *Sur un théorème de F. Proth*, Mat. Vesnik 1(16) (1964), pp. 243–244.

[18] E. Trost, *Primzahlen*, Basel–Stuttgart, 1953, p. 38.

[19] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. 62 (1955), pp. 230–236.

[20] C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr., *The pseudoprimes to $25\cdot 10^9$*, to appear in Math. Comp.

INSTITUTE OF MATHEMATICS, POLISH ACADEMY OF SCIENCES
DEPARTMENT OF MATHEMATICS AND NATURAL SCIENCES
WARSAW UNIVERSITY DIVISION, Białystok, Poland

INSTITUT MITTAG-LEFFLER, SWEDISH ACADEMY OF SCIENCES
Auravägen 17, S-18262 Djursholm, Sweden

Received on 31.12.1976
and in revised form on 12.11.1977 (905)