ON THE THEOREM OF WÓJCIK

by A. ROTKIEWICZ

Dedicated to the memory of my friend Jan Wójcik (1936–1994)

(Received 13 October, 1994)

In the paper **[3]** the following lemma was proved.

LEMMA. *Let a, b and c be positive integers such that a and bc are relatively prime. Then there are infinitely many primes p in the arithmetic progression $ax+b$ ($x = 0, 1, 2, \ldots$) such that*

$$p \mid (2^{(p-1)/c} - 1).$$

In 1982 Jan Wójcik proved **[10]** a similar result about the so called Lehmer numbers. Lehmer numbers can be defined as follows:

$$P_n(\alpha, \beta) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{if } n \text{ is odd,} \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{if } n \text{ is even,} \end{cases}$$

where α, β roots of the trinomial $z^2 - \sqrt{L}\, z + M$, its discriminant is $D = L - 4M$ and $L > 0$ and M are rational integers. We can assume without any essential loss of generality that $(L, M) = 1$.

Put for the moment $P'_n = P_n(\alpha, \beta)$. Lehmer numbers can be also defined as follows

$$P'_1 = P'_2 = 1,$$

$$P'_n = \begin{cases} LP'_{n-1} - MP'_{n-2} & \text{if } n \text{ is odd,} \\ P'_{n-1} - MP'_{n-2} & \text{if } n \text{ is even.} \end{cases}$$

In 1982 Jan Wójcik **[10]** proved the following

THEOREM W. *If α, β defined above are different from zero and α/β is not a root of unity then there exists a positive integer k_0 such that for every positive integer k divisible by k_0 and for all positive integers a and b, where $(a, b) = 1$ and $b \equiv 1(\mathrm{mod}(a, k))$, there exist infinitely many primes satisfying the conditions*

$$p \equiv b(\mathrm{mod}\, a), \qquad p \equiv 1(\mathrm{mod}\, k), \qquad p \mid P_{(p-1)/k}(\alpha, \beta). \tag{1}$$

REMARK. For any α, β in Theorem W, the constant $k_0 = k_0(\alpha, \beta)$ may be given explicitly **[11]**. For example, for the Fibonacci sequence, $k_0 = 20$.

Here we shall prove a similar result for composite numbers. Let

$$V_n = \begin{cases} (\alpha^n + \beta^n)/(\alpha + \beta) & \text{if } n \text{ is odd,} \\ (\alpha^n + \beta^n) & \text{if } n \text{ is even,} \end{cases}$$

denote the nth term of the associated Lehmer recurring sequence. The associated Lehmer sequence V_k can be defined as follows: $V_0 = 2$, $V_1 = 1$, and for $n \geq 2$

$$V_n = \begin{cases} LV_{n-1} - MV_{n-2} & \text{for } n \text{ even,} \\ V_{n-1} - MV_{n-2} & \text{for } n \text{ odd.} \end{cases}$$

An odd composite number n is a *strong Lehmer pseudoprime with parameters* L, M (*or for the bases* α *and* β) if $(n, DL)=1$ and with $n-(DL/n)=d\,.\,2^s$, d odd, where (DL/n) is the Jacobi symbol, we have either

(i) $$P_d \equiv 0 (\bmod n), \quad \text{or}$$

(ii) $$V_{d.2^r} \equiv 0 (\bmod n), \quad \text{for some } r \text{ with } \quad 0 \le r < s.$$

Every odd prime n satisfies (i) or (ii) provided $(n, DL)=1$ (cf. [**6**]).

In 1994 I proved [**6**] the following

THEOREM T. *If α, β defined above are different from zero and α/β is not a root of unity (that is $\langle L, M\rangle \neq \langle 1,1\rangle, \langle 2,1\rangle, \langle 3,1\rangle$) then every arithmetical progression $ax+b(x=0,1,2,\ldots)$, where a, b are relatively prime positive integers, contains an infinite number of odd strong Lehmer pseudoprimes for the bases α and β.*

In 1982 I proved [**5**] this theorem only in the case $D=(\alpha-\beta)^2>0$. We shall introduce the following

DEFINITION. Let $P_n(\alpha, \beta)$ denote the nth Lehmer number. An odd composite n is a *kth order strong Lehmer pseudoprime for the bases α and β* if $(n, DL)=1$ and, with $n-(DL/n)\equiv 0(\bmod k)$, $d=\dfrac{1}{k}(n-(DL/n))$, $(d,k)=1$, we have

$$P_d(\alpha, \beta) \equiv 0 (\bmod n). \tag{2}$$

For $k=2^s$ we get a strong Lehmer pseudoprime satisfying (i), for the bases α and β.

Now we shall prove the following

THEOREM W_1. *Let $P_n(\alpha, \beta)$ denote the nth Lehmer number. If α/β is not a root of unity then there exists a positive integer k_0 such that for every positive integer k divisible by k_0 and for all positive integers a and b, where $(a,b)=1$ and $b\equiv 1+k(\bmod k^2)$, in every arithmetical progression $ax+b$ $(x=0,1,2,\ldots)$ there exist infinitely many kth order strong Lehmer pseudoprimes for the bases α and β.*

For each positive integer n we denote by $\phi_n(\alpha, \beta)=\bar{\phi}_n(L, M)$ the nth cyclotomic polynomial

$$\bar{\phi}_n(L, M)=\phi_n(\alpha, \beta)=\prod_{(m,n)=1}(\alpha-\zeta_n^m\beta),$$

where ζ_n is a primitive nth root of unity and the product is over the $\varphi(n)$ integers m with $1\le m\le n$ and $(m,n)=1$.

It will be convenient to write

$$\phi(\alpha, \beta; n)=\phi_n(\alpha, \beta).$$

It is easy to see that $\phi(\alpha, \beta; n)>1$ for $D=L-4M>0$, $n>2$. A prime factor p of $P_n=P_n(\alpha, \beta)$ is called a primitive factor of P_n if $p\mid P_n$ but $p\nmid DLP_3\ldots P_{n-1}$.

Assume that $M\neq 0$, $D=L-4M\neq 0$, $\langle L, M\rangle \neq \langle 1,1\rangle, \langle 2,1\rangle, \langle 3,1\rangle$; (i.e. β/α is not a root of unity).

The following results are well known.

LEMMA 1. (Lehmer [2]). *Let* $n \neq 2^\gamma, 3\,.\,2^\gamma$. *Denote by* $r = r(n)$ *the largest prime factor of* n. *If* $r \nmid \phi(\alpha, \beta; n)$, *then every prime* p *dividing* $\phi(\alpha, \beta; n)$ *is a primitive prime divisor of* P_n.

Every primitive prime divisor p *of* P_n *is* $\equiv(DL/p)(\mathrm{mod}\, p)$. *If* $r \mid \phi(\alpha, \beta; n)$, $r^l \,\|\, n$ (*which is to say* $r^l \mid n$ *but* $r^{l+1} \nmid n$) *then* $r \,\|\, \phi(\alpha, \beta; n)$ *and* r *is a primitive prime divisor of* P_{n/r^l}.

LEMMA 2. *The number* P_n *for* $n > 12$, $D > 0$ *has a primitive prime divisor* (see Durst [1], Ward [9]). *If* $D < 0$ *and* β/α *is not a root of unity, then, for* $n > n_0(\alpha, \beta)$, P_n *has a primitive prime divisor. The number* $n_0(\alpha, \beta)$ *can be effectively computed* (Schinzel [7]); $n_0 = n_0(\alpha, \beta) = e^{452}\,.\,4^{67}$ (Stewart [8]). *We have* $|\phi(\alpha, \beta; n)| > 1$ *for* $n > n_0$ ([7], [8]).

LEMMA 3. (Rotkiewicz [4, Lemma 5]). *Let*

$$\psi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) = 2 p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} (p_1^2 - 1)(p_2^2 - 1) \dots (p_k^2 - 1).$$

If q *is a prime such that* $q^2 \,\|\, n$ *and* a *is a natural number such that* $a\psi(a) \mid (q-1)$, *then* $\phi(\alpha, \beta; n) \equiv 1(\mathrm{mod}\, a)$.

Proof of Theorem W_1. It is sufficient to show that there exists one kth order strong Lehmer pseudoprime for the bases α and β of the form $ax + b$. To see this just notice that we then have such pseudoprimes of the shape $adx + b$ for every natural d with $(d, b) = 1$ and we may choose d as large as we wish. We may also suppose without loss of generality that b is odd and that $4DL \mid a$, since if b_1 is prime of the form $k^2at + b$, then every term of the progression $k^2at + b_1$ $(t = 1, 2, \dots)$ is $\equiv b(\mathrm{mod}\, a)$, its difference is k^2a and $(k^2a, b_1) = 1$.

Let $DLk_0 \mid k$ where k_0 is an integer from the theorem of Wójcik. We have $b_1 = k^2at + b \equiv 1 + k(\mathrm{mod}\, k^2)$. Now let p_1, p_2, p_3, p_4 be different primes such that $(p_1 p_2 p_3 p_4, ak) = 1$ and let q be a prime number such that

$$c\psi(c) \mid q - 1, \qquad c = k^2 a p_1 p_2 p_3 p_4. \tag{3}$$

Let m be a positive integer such that

$$\begin{aligned} m &\equiv b(\mathrm{mod}\, ak^2), \\ m &\equiv 1 + p_1 p_2 p_3 p_4 q^2 (\mathrm{mod}\, p_1^2 p_2^2 p_3^2 p_4^2 q^3). \end{aligned} \tag{4}$$

Such positive m exists by the Chinese Remainder Theorem. From (4) and $b \equiv 1 + k(\mathrm{mod}\, k^2)$, it follows that

$$(m, ak^2 p_1^2 p_2^2 p_3^2 p_4^2 q^3) = 1.$$

Since $m \equiv b \equiv 1 + k(\mathrm{mod}\, k^2)$ we have $m \equiv 1(\mathrm{mod}\, k)$. Thus also $m \equiv 1(\mathrm{mod}(k^2 a p_1^2 p_2^2 p_3^2 p_4^2 q^2, k))$ and by, Theorem W, there exist infinitely many primes p in the arithmetical progression $k^2 a p_1^2 p_2^2 p_3^2 p_4^2 q^3 x + m (x = 1, 2, \dots)$ for which

$$P_{(p-1)/k}(\alpha, \beta) \equiv 0(\mathrm{mod}\, p).$$

Let p be one of them. From $4DLk_0 \mid k$, $m \equiv 1(\mathrm{mod}\, k)$ it follows that $m \equiv 1(\mathrm{mod}\, 4DL)$, hence $(DL/m) = 1$ and also $(DL/p) = 1$. We have that $(p-1)/k \equiv (m-1)/k \equiv 1(\mathrm{mod}\, k)$, hence $((p-1)/k, k) = 1$.

Let $\bar{r}$ denote the greatest prime factor of $p - 1$. It is easy to see that one of numbers

https://doi.org/10.1017/S0017089500031384 Published online by Cambridge University Press

$\phi(\alpha, \beta; (p-1)/kp_i)$ for $i = 1, 2, 3, 4$ can be divisible by $\bar{r}$ and only one can be divisible by p. Without loss of generality we can assume that $p \nmid \phi(\alpha, \beta; (p-1)/kp_i)$ and $\bar{r} \nmid \phi(\alpha, \beta; (p-1)/kp_i)$ for $i = 1, 2$.

Let $m_i = \phi\left(\alpha, \beta; \dfrac{p-1}{kp_i}\right)$ for $i = 1, 2$. Now we shall prove that if $m_1 > 0$ or $m_2 > 0$ then pm_1 or pm_2 is our required pseudoprime and if $m_1 < 0$ and $m_2 < 0$ then pm_1m_2 is our required pseudoprime. First we shall consider the case when $m_1 > 0$ or $m_2 > 0$.

Suppose for example that $m_1 > 0$. Let $s_1 = \dfrac{p-1}{kp_1}$. By Lemma 1 every prime factor t of m_1 is congruent to $(DL/t)(\text{mod}\, s_1)$. Since $m_1 > 0$, by Lemma 2, m_1 is a positive integer greater than 1. So

$$m_1 \equiv (DL/m_1)(\text{mod}\, s_1). \tag{5}$$

Certainly $q^2 \| s_1 = (p-1)/kp_1$. So from $a\psi(a) \mid (q-1)$, $4DL \mid a$, by Lemma 3 we have $m_1 \equiv 1(\text{mod}\, 4DL)$. So $(DL/m_1) = 1$ and from (5) it follows that

$$m_1 \equiv 1(\text{mod}\, s_1), \qquad s_1 = \frac{p-1}{kp_1}. \tag{6}$$

Further, from $q^2 \| s_1$, $kp_1\psi(kp_1) \mid (p-1)$, by Lemma 3 we have

$$m_1 \equiv 1(\text{mod}\, kp_1). \tag{7}$$

Since $p \equiv 1 + k(\text{mod}\, k^2)$ and $p \equiv 1 + p_1p_2p_3p_4q^2(\text{mod}\, p_1^2)$, we have $(s_1, kp_1) = 1$. Thus from (6) and (7) we get

$$m_1 \equiv 1(\text{mod}\, (p-1)), \tag{8}$$

and $n_1 = pm_1 \equiv 1(\text{mod}(p-1))$; hence

$$(n_1 - 1)/k \equiv 0(\text{mod}(p-1)/k). \tag{9}$$

From $k^2\psi(k^2) \mid (q-1)$, $q^2 \mid (p-1)/k$, by Lemma 3 we get

$$m_1 \equiv 1(\text{mod}\, k^2); \tag{10}$$

hence $n_1 = pm_1 \equiv (1+k)1 \equiv 1 + k(\text{mod}\, k^2)$ and

$$((n_1 - 1)/k, k) = 1. \tag{11}$$

Further, $(DL/n_1) = (DL/pm_1) = (DL/p)(DL/m_1) = 1 \,.\, 1 = 1$. Thus from (9) and (11) we get

$$m_1 = \phi(\alpha, \beta; (p-1)/kp_1) \mid P_{(p-1)/k} \mid P_{(n_1-1)/k} = P_{(n_1-(DL/n_1))/k}, \tag{12}$$

where $((n_1 - (DL/n_1))/k, k) = 1$, $P_i = P_i(\alpha, \beta)$.

Also

$$p \mid P_{(p-1)/k} \mid P_{(n_1-(DL/n_1))/k}. \tag{13}$$

Since $(p_1, m_1) = 1$, by (12) and (13) we have

$$n_1 = pm_1 \mid P_{(n_1-(DL/n_1))/k}.$$

Since $m_1 \equiv 1(\mathrm{mod}\, a)$ we have

$$n_1 = pm_1 \equiv b\,.\,1 \equiv b(\mathrm{mod}\, a) \tag{14}$$

as required.

If the both numbers m_1 and m_2 are negative their product m_{12} is positive and

$$m_{12} \equiv (DL/m_{12})(\mathrm{mod}(p-1)/kp_1p_2), \tag{15}$$

where $m_{12} = m_1m_2$, $m_i = \phi(\alpha, \beta; (p-1)/kp_i$ for $i = 1, 2$.

Indeed, let $m_{12} = q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_l^{\alpha_l}$. By Lemma 1 we have

$$q_i^{\alpha_i} \equiv (DL/q_i)^{\alpha_i}(\mathrm{mod}(p-1)/kp_1p_2).$$

Thus

$$\begin{aligned} m_{12} &\equiv (DL/q_1)^{\alpha_1}(DL/q_2)^{\alpha_2}\ldots(DL/q_l)^{\alpha_l} \equiv (DL/q_1^{\alpha_1})(DL/q_2^{\alpha_2})\ldots(DL/q_l^{\alpha_l}) \\ &\equiv (DL/m_{12})(\mathrm{mod}(p-1)/kp_1p_2). \end{aligned}$$

Certainly $q^2 \,\|\, (p-1)/kp_1p_2$ and $a\psi(a) \mid q-1$ and by Lemma 3, $m_1 \equiv 1(\mathrm{mod}\, a)$ for $i = 1, 2$; hence we have $m_{12} \equiv 1(\mathrm{mod}\, a)$.

Since $4DL \mid a$, we have $m_{12} \equiv 1(\mathrm{mod}\, 4DL)$. So $(DL/m_{12}) = 1$ and from (15) we get

$$m_{12} \equiv 1(\mathrm{mod}(p-1)/kp_1p_2). \tag{16}$$

From $p_1p_2\psi(p_1p_2) \,\|\, (q-1)$, $q^2 \,\|\, (p-1)/kp_1p_2$, by Lemma 3 we have $m_i \equiv 1(\mathrm{mod}\, p_1p_2)$ for $i = 1, 2$; hence

$$m_{12} \equiv 1(\mathrm{mod}\, p_1p_2). \tag{17}$$

Since $p_1 \,\|\, (p-1)$, $p_2 \,\|\, (p-1)$, from (16) and (17) we get

$$m_{12} \equiv 1(\mathrm{mod}(p-1)/k). \tag{18}$$

From $k^2\psi(k^2) \mid (q-1)$, $q^2 \,\|\, (p-1)/kp_i$, by Lemma 3 we get $m_i \equiv 1(\mathrm{mod}\, k^2)$; hence $m_{12} = m_1\,.\,m_2 \equiv 1(\mathrm{mod}\, k^2)$, $n_{12} = pm_{12} \equiv 1 + k(\mathrm{mod}\, k^2)$. Hence $((n_{12}-1)/k, k) = 1$. Also $(DL/n_{12}) = 1$ (recall that $(DL/m_1) = 1$, $p \equiv 1(\mathrm{mod}\, 4DL)$). By Lemma 2, $m_{12} > 1$ and

$$m_{12} = \phi(\alpha, \beta; (p-1)/kp_1)\,.\,\phi(\alpha, \beta; (p-1)/kp_2) \mid P_{(p-1)/k} \mid P_{(n_{12}-1)/k} = P_{(n_{12}-(DL/n_{12}))/k}.$$

Also

$$p \mid P_{(p-1)/k} \mid P_{(n_{12}-(DL/n_{12}))/k}$$

and since $(p, m_{12}) = 1$ we have

$$n_{12} = m_{12}p \mid P_{(n_{12}-(DL/n_{12}))/k},$$

where

$$(n_{12} - (DL/n_{12}))/k, k) = 1 \quad \text{and} \quad n_{12} = pm_{12} \equiv a\,.\,1 \equiv b(\mathrm{mod}\, a)$$

as required.

REFERENCES

1. L. K. Durst, Exceptional real Lehmer sequences, *Pacific J. Math.* **9** (1959), 437–441.

2. D. H. Lehmer, An extended theory of Lucas functions, *Ann. Math.* (2) **31** (1930), 419–448.

3. A. Rotkiewicz, On the prime factors of the number $2^{p-1}-1$, *Glasgow Math. J.* **9** (1968), 83–86.

4. A. Rotkiewicz, On the pseudoprimes of the form $ax+b$ with respect to the sequence of Lehmer, *Bull. Acad. Polon. Sci. Ser. Sci. Math. Astronom. Phys.* **20** (1972), 349–354.

5. A. Rotkiewicz, On Euler Lehmer pseudoprimes and strong Lehmer pseudoprimes with parameters L, Q in arithmetic progressions, *Math. Comp.* **39** (1982), 239–247.

6. A. Rotkiewicz, On strong Lehmer pseudoprimes in the case of negative discriminant in arithmetic progression, *Acta Arith.* **68** (1994), 145–151.

7. A. Schinzel, The intrinsic divisors of Lehmer numbers in the case of negative discriminant, *Ark. Math.* **4** (1962), 413–416.

8. C. L. Stewart, Primitive divisors of Lucas and Lehmer numbers, *Transcendence Theory: Advances and Application* (Academic Press, 1977), 79–92.

9. M. Ward, The intrinsic divisors of Lehmer numbers, *Ann. Math.* (2) **62** (1955), 230–236.

10. J. Wójcik, Contribution to the theory of Kummer extension, *Acta Arith.* **40** (1982), 155–174.

11. J. Wójcik, On the density of some sets of primes connected with cyclotomic polynomials, *Acta Arith.* **41** (1982), 117–131.

INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
UL. ŚNIADECKICH 8
00-950 WARSZAWA, POLAND

AND

TECHNICAL UNIVERSITY IN BIAŁYSTOK
UL. WIEJSKA 45, 15-351 BIAŁYSTOK, POLAND