ACTA ARITHMETICA
LXVIII.2 (1994)

On strong Lehmer pseudoprimes in the case of negative discriminant in arithmetic progressions

by

A. Rotkiewicz (Warszawa)

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

The Lehmer sequence P_k is defined recursively as follows: $P_0=0$, $P_1=1$, and for $n\geq 2$,

$$P_n=\begin{cases}LP_{n-1}-MP_{n-2} & \text{if } n \text{ is odd},\\ P_{n-1}-MP_{n-2} & \text{if } n \text{ is even}.\end{cases}$$

Let $V_n=(\alpha^n+\beta^n)/(\alpha+\beta)$ for n odd, and $V_n=\alpha^n+\beta^n$ for n even denote the nth term of the associated recurring sequence.

The associated Lehmer sequence V_k can be defined recursively 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 an *sLp for the bases* α *and* β) if $(n,DL)=1$, and with $\delta(n)=n-(DL/n)=d\cdot 2^s$, d odd, where (DL/n) is the Jacobi symbol, we have either

(i) $P_d\equiv 0 \pmod n$, or
(ii) $V_{d\cdot 2^r}\equiv 0 \pmod n$, for some r with $0\leq r<s$.

Each odd prime n satisfies either (i) or (ii), provided $(n,DL)=1$ (cf. [2]).

In 1982 I proved [4] that if $D = L - 4M > 0$ and $L > 0$ then every arithmetic progression $ax+b$ ($x = 0, 1, 2, \ldots$), where a, b are relatively prime integers, contains an infinite number of odd strong Lehmer pseudoprimes with parameters L, M (that is, sLp's for the bases α and β). In the present paper we prove 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 arithmetic progression $ax + b$* ($x = 0, 1, 2, \ldots$), *where a, b are relatively prime integers*, *contains an infinite number of odd strong Lehmer pseudoprimes for the bases α and β.*

In comparison with [4] the novelty of this theorem lies in the case $D < 0$.

An odd composite n is an *Euler Lehmer pseudoprime for the bases α and β* if $(n, MD) = 1$ and

$$P_{(n-\varepsilon(n))/2} \equiv 0 \pmod{n} \quad \text{if } (ML/n) = 1, \text{ or}$$
$$V_{(n-\varepsilon(n))/2} \equiv 0 \pmod{n} \quad \text{if } (ML/n) = -1, \text{ where } \varepsilon(n) = (DL/n).$$

If n is a strong Lehmer pseudoprime for the bases α and β, then it is an Euler Lehmer pseudoprime for the bases α and β (cf. [4], Theorem 1); thus if the assumptions of Theorem T hold, then every arithmetic progression $ax + b$ ($x = 0, 1, 2, \ldots$), where a, b are relatively prime integers, contains an infinite number of odd Euler Lehmer pseudoprimes for the bases α and β.

2. For each positive integer n we denote by $\Phi_n(\alpha, \beta) = \overline{\Phi}_n(L, M)$ the nth cyclotomic polynomial

$$\overline{\Phi}(L, M) = \Phi_n(\alpha, \beta) = \prod_{(m,n)=1} (\alpha - \zeta_n^m \beta) = \prod_{d\mid n} (\alpha^d - \beta^d)^{\mu(n/d)},$$

where ζ_n is a primitive nth root of unity and the product is over the $\varphi(n)$ integers m with $1 \leq m \leq n$ and $(m, n) = 1$; μ and φ are the Möbius and Euler functions respectively.

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 $D = L - 4M > 0$ and $n > 2$.

A. Schinzel [5] proved that if α and β are complex and β/α is not a root of unity, then for every $\varepsilon > 0$ and $n > N(\alpha, \beta, \varepsilon)$,

$$|\Phi(\alpha, \beta; n)| > |\alpha|^{\varphi(n) - 2^{\nu(n)} \log^{2+\varepsilon} n},$$

where $\nu(n)$ the number of prime factors of n and $N(\alpha, \beta, \varepsilon)$ can be effectively computed.

M. Ward [7] proved that $\Phi(\alpha, \beta; n) > n$ for $n > 12$ and $D > 0$.

A prime factor p of $P_n(\alpha,\beta)$ is called a *primitive prime factor* of P_n if $p \mid P_n$ but $p \nmid DLP_3 \dots P_{n-1}$.

The following results are well known.

LEMMA 1 (Lehmer [2]). *Let $n \neq 2^g, 3\cdot 2^g$. 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 $\equiv (DL/p) \pmod{n}$.*

If $r \mid \Phi(\alpha,\beta;n)$ and $r^l \parallel n$ (that is, $r^l \mid n$ but $r^{l+1} \nmid n$) then $r \parallel \Phi(\alpha,\beta;n)$ and r is a primitive prime divisor of P_{n/r^l}.

LEMMA 2. *For $n > 12$ and $D > 0$ the number P_n has a primitive prime divisor* (see Durst [1], Ward [7]).

If $D < 0$ and β/α is not a root of unity, then P_n has a primitive prime divisor for $n > n_0(\alpha,\beta)$. Here $n_0(\alpha,\beta)$ can be effectively computed (Schinzel [5]); *in fact, $n_0 = n_0(\alpha,\beta) = e^{452}\cdot 4^{67}$* (Stewart [6]).

We have $|\Phi(\alpha,\beta;n)| > 1$ for $n > n_0$ (Schinzel [5], Stewart [6]).

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

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

If q is a prime such that $q^2 \parallel n$ and a is a natural number with $a\Psi(a) \mid q-1$, then $\Phi(\alpha,\beta;n) \equiv 1 \pmod{a}$.

3. Proof of Theorem T. The case $D > 0$ is considered in [4], so we assume that $D < 0$.

If for each pair of relatively prime integers a, b there is at least one strong Lehmer pseudoprime with parameters L, M of the shape $ax+b$, where x is a natural number, then there are infinitely many such pseudoprimes. We may suppose without loss of generality that a is even and b is odd and that $4DL \mid a$.

The proofs of the above results are the same as in the case $D > 0$. Thus, the theorem will be proved if we can produce a strong Lehmer pseudoprime n with parameters L, M with $n \equiv b \pmod{a}$.

Given a and b as described, with $2^\lambda \parallel b - (DL/b)$, $\lambda \geq 1$, we start our construction by choosing four distinct primes p_1, p_2, p_3, p_4 that are relatively prime to a. Furthermore, we introduce two further primes p and q, with $q > p_i$ $(i = 1,2,3,4)$, which are to satisfy certain conditions detailed below. Firstly, we require that

(a) $$2^\lambda p_1p_2p_3p_4q^2 \parallel p - \varepsilon(p), \quad \varepsilon(p) = (DL/p), \quad (DL,p) = 1.$$

We apply Dirichlet's theorem on primes in arithmetic progressions to select a prime q with

(1) $$2p_1p_2p_3p_4(p_1^2-1)(p_2^2-1)(p_3^2-1)(p_4^2-1) \mid q-1, \quad 3\cdot 2^{2\lambda+3}a\Psi(a) \mid q-1.$$

Then automatically we have $q > p_i$ $(i = 1,2,3,4)$. Since $(a,b) = 1$ and $4DL \mid a$, we have $(DL/b) \neq 0$.

By the Chinese Remainder Theorem there exists a natural number m such that

$$(2)\quad m \equiv (DL/b) + p_1p_2p_3p_4q^2 \pmod{p_1^2p_2^2p_3^2p_4^2q^3}, \quad m \equiv b \pmod{2^{\lambda+1}a}.$$

From (2) it follows that $(m, 2ap_1^2p_2^2p_3^2p_4^2q^3) = 1$ and by Dirichlet's theorem, there exists a positive x such that

$$2^{\lambda+1}ap_1^2p_2^2p_3^2p_4^2q^3x + m = p \quad \text{is a prime.}$$

Since $4DL \mid a$, we have $p \equiv m \pmod{4DL}$, hence

$$\varepsilon(p) = (DL/p) = (DL/m) = (DL/b).$$

Thus $2^\lambda p_1p_2p_3p_4q^2 \parallel p - \varepsilon(p)$ and $(DL,p) = 1$. This gives (a).

Since p is prime, it satisfies the conditions

$$P_d \equiv 0 \pmod{p} \quad \text{or} \quad V_{2^rd} \equiv 0 \pmod{p}$$

for some r, $0 \le r < \lambda$, with

$$p - \varepsilon(p) = 2^\lambda d, \quad \varepsilon(p) = (DL/p).$$

So

$$(3)\quad \text{either} \quad P_{(p-\varepsilon(p))/2^\lambda} \equiv 0 \pmod{p} \quad \text{or} \quad V_{(p-\varepsilon(p))/2^\mu} \equiv 0 \pmod{p}$$

for some μ, $0 < \mu \le \lambda$.

Our considerations rest on the fact that only one of the numbers $m_i = \Phi(\alpha,\beta;(p-(DL/p))/2^\nu p_i)$ $(1 \le i \le 4)$ is divisible by p and only one of them is divisible by the highest prime factor $\bar r$ of $p - (DL/p)$.

Indeed, let $s_i = (p-\varepsilon(p))/2^\nu p_i$. We can assume that $s_i > n_0(\alpha,\beta)$, so by Lemma 2, P_{s_i} has a primitive prime divisor. Hence if p divided more than one of the m_i, then by Lemma 1, p would be a primitive prime factor of both P_{s_i} and P_{s_j}, which is absurd if $s_i \neq s_j$. So we may suppose that p divides neither m_1 nor m_2 nor m_3. By (a) we have $\bar r \le q$, so $\bar r > p_1,p_2,p_3,p_4$ and thus $\bar r$ is the greatest prime divisor of s_1, s_2 and s_3. Again by Lemma 1, if $\bar r$ were to divide both m_2 and m_3, then $\bar r$ would be a primitive prime factor of both $P_{s_2/\bar r^k}$ and $P_{s_3/\bar r^k}$, where $\bar r^k \| p-\varepsilon(p)$. But this is absurd, so without loss of generality $\bar r$ does not divide m_2 and m_1.

Thus without loss of generality one can assume that neither $m_1 = \Phi(\alpha,\beta;(p-(DL/p))/2^\nu p_1)$ nor $m_2 = \Phi(\alpha,\beta;(p-(DL/p))/2^\nu p_2)$ is divisible by p or $\bar r$.

Now the proof of Theorem T can be divided into four cases:

(i) the first alternative of (3) holds with $m_1 > 0$ or $m_2 > 0$ (where $\nu = \lambda$),

(ii) the second alternative of (3) holds for some $0 < \mu \le \lambda$ with $m_1 > 0$ or $m_2 > 0$ (where $\nu = \mu - 1$),

(iii) the first alternative of (3) holds, but m_1, $m_2 < 0$ (where $\nu = \lambda$),

(iv) the second alternative of (3) holds for some $0 < \mu \le \lambda$ with m_1, $m_2 < 0$ (where $\nu = \mu - 1$).

By Lemma 2 we can assume that

$$|\Phi(\alpha,\beta;(p-\varepsilon(p))/2^\nu p_i)| > 1$$

where $\nu = \lambda$ or $\nu = \mu - 1$ and $i = 1, 2$.

It will be convenient to write

$$n_i = pm_i \quad (i = 1,2), \quad m_{12} = m_1 m_2, \quad n_{12} = pm_1 m_2.$$

In case (i) without loss of generality we can assume that $m_1 > 0$, and $n_1 = p\Phi(\alpha,\beta;(p-\varepsilon(p))/2^\lambda p_1)$ is the required strong Lehmer pseudoprime. The proof is the same as in the case $D > 0$ (cf. [4]).

In case (ii) also without loss of generality we can assume that $m_1 > 0$, and $n_1 = p\cdot\Phi(\alpha,\beta;(p-\varepsilon(p))/2^{\mu-1} p_1)$ is the required strong Lehmer pseudoprime of the form $ax + b$. The proof is the same as in the case $D > 0$ (cf. [4]).

In case (iii),

$$n_{12} = p \cdot \Phi(\alpha,\beta;(p-\varepsilon(p))/2^\lambda p_1) \cdot \Phi(\alpha,\beta;(p-\varepsilon(p))/2^\lambda p_2)$$

is the required strong Lehmer pseudoprime.

Indeed, since $\bar{r}$ does not divide m_1 and m_2, Lemma 1 implies that every prime factor t of m_1 is congruent to (DL/t) mod s_1 or s_2, hence is congruent to (DL/t) mod $(p-\varepsilon(p))/2^\lambda p_1 p_2$.

Since $m_{12} = \Phi(\alpha,\beta;(p-\varepsilon(p))/2^\lambda p_1) \cdot \Phi(\alpha,\beta;(p-\varepsilon(p))/2^\lambda p_2) > 0$ we have

$$m_{12} \equiv (DL/m_{12}) \pmod{(p-\varepsilon(p))/2^\lambda p_1 p_2}, \tag{4}$$

where $m_{12} = m_1 m_2$ with $m_i = \Phi(\alpha,\beta;(p-\varepsilon(p))/2^\lambda p_i)$ for $i = 1, 2$.

Certainly $q^2 \parallel (p-\varepsilon(p))/2^\lambda p_1 p_2$ and $a\Psi(a) \mid q-1$. By Lemma 3, $m_i \equiv 1 \pmod{a}$ for $i = 1, 2$, hence we have $m_{12} \equiv 1 \pmod{a}$. Since $4DL \mid a$, we obtain $m_{12} \equiv 1 \pmod{4DL}$. So $(DL/m_{12}) = 1$ and from (4) it follows that

$$m_{12} \equiv 1 \pmod{(p-\varepsilon(p))/2^\lambda p_1 p_2}. \tag{5}$$

Since $p_1 p_2 \Psi(p_1 p_2) \mid q-1$ and $q^2 \parallel (p-\varepsilon(p))/2^\lambda p_1 p_2$, by Lemma 3 we have $m_i \equiv \pmod{p_1 p_2}$ for $i = 1, 2$, hence

$$m_{12} \equiv 1 \pmod{p_1 p_2}. \tag{6}$$

The requirement on q that $3\cdot 2^{2\lambda+3} \mid q-1$ implies by Lemma 3 (recall that $2^{\lambda+1}\Psi(2^{\lambda+1}) = 3\cdot 2^{2\lambda+3}$ and $q^2 \parallel (p-\varepsilon(p))/2^\lambda p_1 p_2$) that $m_i \equiv 1 \pmod{2^{\lambda+1}}$

for $i = 1, 2$, hence

$$m_{12} = 1 \pmod{2^{\lambda+1}}. \tag{7}$$

Recalling $p_1 \parallel p - \varepsilon(p)$, $p_2 \parallel p - \varepsilon(p)$ and $2^\lambda \parallel p - \varepsilon(p)$, we conclude from (5), (6) and (7) that

$$m_{12} \equiv 1 \pmod{2(p - \varepsilon(p))},$$

which says that

$$n_{12} = pm_{12} = p(2(p - \varepsilon(p))\overline{x} + 1) = (p - \varepsilon(p))(2p\overline{x} + 1) + \varepsilon(p) \tag{8}$$

for some positive $\overline{x}$; n_{12} is positive because $\Phi(\alpha, \beta, s_1) \cdot \Phi(\alpha, \beta, s_2) > 1$ for $s_i > n_0(\alpha, \beta)$, by Lemma 2.

Now we use the first alternative of (3). We have

$$\varepsilon(n_{12}) = (DL/pm_1m_2) = (DL/p) \cdot (DL/m_1m_2) = (DL/p) \cdot 1 = \varepsilon(p). \tag{9}$$

By (9) we have

$$\frac{n_{12} - \varepsilon(n_{12})}{2^\lambda} = \frac{n_{12} - \varepsilon(p)}{2^\lambda} = \frac{p - \varepsilon(p)}{2^\lambda}(2p\overline{x} + 1)$$

and

$$m_{12} = \Phi(\alpha, \beta; (p - \varepsilon(p))/2^\lambda p_1) \cdot \Phi(\alpha, \beta; (p - \varepsilon(p))/2^\lambda p_2) \mid P_{(p-\varepsilon(p))/2^\lambda}.$$

Moreover, $p \mid P_{(p-\varepsilon(p))/2^\lambda}$, $(p, m_{12}) = 1$. Hence

$$n_{12} = pm_{12} \mid P_{(p-\varepsilon(p))/2^\lambda} \mid P_{(n_{12}-\varepsilon(n_{12}))/2^\lambda},$$

where $(n_{12} - \varepsilon(n_{12}))/2^\lambda$ is odd. Hence n_{12} is an sLp with parameters L, M.

In case (iv),

$$n_{12} = p\Phi(\alpha, \beta; (p - \varepsilon(p))/2^{\mu-1}p_1) \cdot \Phi(\alpha, \beta; (p - \varepsilon(p))/2^{\mu-1}p_2)$$

is the required strong Lehmer pseudoprime. We have, as before,

$$\frac{n_{12} - \varepsilon(n_{12})}{2^\mu} = \frac{p - \varepsilon(p)}{2^\mu}(2px + 1)$$

and we note that $2px + 1$ is odd. Hence

$$m_{12} = \Phi(\alpha, \beta; (p - \varepsilon(p))/2^{\mu-1}p_1) \cdot \Phi(\alpha, \beta; (p - \varepsilon(p))/2^{\mu-1}p_2) \mid V_{(p-\varepsilon(p))/2^\mu},$$

$p \mid V_{(p-\varepsilon(p))/2^\mu}$ and since $(p, m_{12}) = 1$ we have

$$n_{12} = p\Phi(\alpha, \beta; (p - 1)/2^{\mu-1}p_1) \cdot \Phi(\alpha, \beta; (p - 1)/2^{\mu-1}p_2) \mid V_{(p-\varepsilon(p))/2^\mu} \mid V_{(n_{12}-\varepsilon(n_{12}))/2^\mu}$$

so also in this case n_{12} is an sLp with parameters L, M.

These remarks conclude the proof for we have $a\Psi(a) \mid q - 1$ and $q^2 \parallel (p - \varepsilon(p))/p_1p_2$, so Lemma 3 yields $m_{12} \equiv 1 \pmod{a}$. Hence $n_{12} = pm_{12} \equiv b \pmod{a}$ 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. of Math. (2) 31 (1930), 419–448.
[3] A. Rotkiewicz, *On the pseudoprimes of the form $ax+b$ with respect to the sequence of Lehmer*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 20 (1972), 349–354.
[4] —, *On Euler Lehmer pseudoprimes and strong Lehmer pseudoprimes with parameters L, Q in arithmetic progressions*, Math. Comp. 39 (1982), 239–247.
[5] A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. 4 (1962), 413–416.
[6] C. L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*, in: Transcendence Theory: Advances and Applications, Academic Press, 1977, 79–92.
[7] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) 62 (1955), 230–236.

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

and

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

Received on 4.8.1993
and in revised form on 13.4.1994 (2470)