Andrzej Rotkiewicz

On Lucas pseudoprimes of the form $ax^2 + bxy + cy^2$ in arithmetic progression $AX + B$ with a prescribed value of the Jacobi symbol

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 10 (2002), No. 1, 103--109

Persistent URL: `http://dml.cz/dmlcz/120575`

On Lucas pseudoprimes of the form $ax^2 + bxy + cy^2$ in arithmetic progression $AX + B$ with a prescribed value of the Jacobi symbol

A. Rotkiewicz

Abstract. For an integer $n \neq 0$, let $\overline{n}$ denote the square-free kernel of n. Let $ax^2 + bxy + cy^2$ be an integral quadratic primitive indefinite form with odd fundamental discriminant $d = b^2 - 4ac$ and belonging to the principal genus.

Let all prime factors of $d > 0$ be of the form $4k + 1$. Let be given integers P, Q with $D = P^2 - 4Q$, $\langle P, Q\rangle \neq \langle 1, 1\rangle$, $(D, d) = 1$ and let $2 \nmid \overline{\alpha\beta} = \overline{Q}$.

If $\varepsilon = \pm 1$, every arithmetic progression $AX + B$, where $(A, B) = 1$, $4D \mid A$, $(A, d\,\overline{\alpha\beta}) = 1$ which contains an odd integer n_0 with $(D/n_0) = \varepsilon$, contains infinitely many Lucas pseudoprimes n with parameters P and Q of the form $ax^2 + bxy + cy^2$ such that $(D/n) = \varepsilon$.

Odd composite numbers n for which $a^{n-1} \equiv 1(\mathrm{mod}\, n)$ are called pseudoprimes to base a.

In the present paper I combine the arguments of [14] and [16] to prove a result on pseudoprimes, which does not follow from the theorems of either paper.

Let P, Q be rational integers $D = P^2 - 4Q$ and

$$U_0 = 0,\ U_1 = 1,\ U_n = PU_{n-1} - QU_{n-2}\ (\text{for } n \geq 2),$$
$$V_0 = 2,\ V_1 = P,\ V_n = PV_{n-1} - QV_{n-2}\ (\text{for } n \geq 2).$$

A composite number n is called a Lucas pseudoprime with parameters P and Q if $(n, 2QD) = 1$ and

$$U_{n-(D/n)} \equiv 0(\mathrm{mod}\, n), \tag{1}$$

where (D/n) is the Jacobi symbol.

Received: November 7, 2001.

2000 *Mathematics Subject Classification:* primary 11A07; secondary 11B39.

Key words and phrases: pseudoprime, Lucas pseudoprime, strong Lucas pseudoprime, Lucas sequences.

A composite number n is called a strong Lucas pseudoprime with parameters P and Q if $(n, 2QD) = 1$, $n - (D/n) = 2^s r$, r odd and

$$\text{(2)} \qquad \text{either} \quad U_r \equiv 0 (\operatorname{mod} n) \quad \text{or} \quad V_{2^t r} \equiv 0 (\operatorname{mod} n)$$

for some t, $0 \leq t < s$.

Efficient primality tests are very important from point of view of cryptography, hence results on pseudoprimes are interesting not only from theoretical but also from practical point of view.

Several previous theorems assert the existence of infinitely many Lucas pseudoprimes [2], [7].

Most of the Lucas pseudoprimes exhibited in proofs of their existence have Jacobi symbol equal to +1 [7].

My construction of Lucas pseudoprimes of the form $ax^2 + bxy + cy^2$ [14] provides pseudoprimes with the Jacobi symbol equal to 1.

In a letter to the present writer C. Pomerance asked whether there are infinitely many Lucas pseudoprimes to any trinomial $x^2 - Px + Q$, where $D = P^2 - 4Q$ is not a square with Jacobi symbol equal to -1 (see also Crandall and Pomerance [4], p. 138).

In [14] we give an affirmative answer to this question with the theorem:

Given integers P, Q with $D = P^2 - 4Q \neq 0, -Q, -2Q, -3Q$ and $\varepsilon = \pm 1$, every arithmetic progression $ax + b$, where $(a, b) = 1$ which contains an odd integer n_0 with $(D/n_0) = \varepsilon$ contains infinitely many strong Lucas pseudoprimes n with parameters P and Q such that $(D/n) = \varepsilon$. The number $N(X)$ of such strong pseudoprimes not exceeding X satisfies

$$N(X) > c(P, Q, a, b, \varepsilon) \frac{\log X}{\log \log X},$$

where $c(P, Q, a, b, \varepsilon)$ is a positive constant depending on P, Q, a, b, ε.

We have

$$U(\alpha, \beta; n) = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

where α and β are distinct roots of the trinomial $f(z) = z^2 - Pz + Q$.

For an integer $n \neq 0$, let $\overline{n}$ denote the square-free kernel of n that is n divided by its greatest square factor.

Here we shall prove the following

Theorem. *Let $ax^2 + bxy + cy^2$ be an integral quadratic primitive indefinite form with odd fundamental discriminant $d = b^2 - 4ac$ and belonging to the principal genus.*

Let all prime factors of $d > 0$ be of the form $4k + 1$.

Let be given integers P, Q with $D = P^2 - 4Q$, $(P, Q) = 1$, $\langle P, Q \rangle \neq \langle 1, 1 \rangle$, $(D, d) = 1$. Let $2 \nmid \overline{\alpha\beta} = \overline{Q}$.

If $\varepsilon = \pm 1$, every arithmetic progression $AX + B$, where $(A, B) = 1$, $4D \mid A$, $(A, d\overline{\alpha\beta}) = 1$ which contains an odd integer n_0 with $(D/n_0) = \varepsilon$, contains infinitely many Lucas pseudoprimes n with parameters P and Q of the form $ax^2 + bxy + cy^2$ such that $(D/n) = \varepsilon$.

For each positive n we denote by $\phi(\alpha, \beta; n)$ the nth cyclotomic polynomial

$$\prod_{(m,n)=1} (\alpha - \zeta_n^m \beta) = \prod_{d|n} (\alpha^d - \beta^d)^{\mu(n/d)},$$

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

We say that a prime p is a primitive prime factor of the number $U(\alpha, \beta; n)$ if p divides $U(\alpha, \beta; n)$ but does not divide $U(\alpha, \beta; 1) \dots U(\alpha, \beta; n-1)$.

In the proof of our theorem we shall use the following Lemmas.

Lemma 1.

a) (Lehmer [8]) *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 $U(\alpha, \beta; n)$.*

   Every primitive prime divisor p of $U(\alpha, \beta; n)$ is $\equiv (D/n) (\operatorname{mod} n)$. If $n \neq r^l$, $2r^l$, $r \mid \phi(\alpha, \beta; n)$ and $r^l \| n$ (which is to say $r^l \mid n$ but $r^{l+1} \nmid n$), r is a primitive prime divisor of $U\left(\alpha, \beta; \frac{n}{r^l}\right)$ and $r \| \phi(\alpha, \beta; n)$.

b) (Durst [6], Ward [20]) *The number $U(\alpha, \beta; n)$ for $n > 12$, $D > 0$ has a primitive divisor and $\phi(\alpha, \beta; n) > n$ for $n > 12$.*

c) (Schinzel [18], Stewart [19]) *If $D < 0$, $(P, Q) = 1$, $\langle P, Q \rangle \neq \langle 1, 1 \rangle$, then $U(\alpha, \beta; n)$ has a primitive prime divisor for $n > n_0$ and $|\phi(\alpha, \beta; n)| > n$ for $n > n_0$.*

Remark. Very recently Bilu, Hanrot and Voutier [3] proved the same statement with the possible $n_0 = 30$.

Lemma 2 (Schinzel [17]). *Let $n > 1$ be square-free and let m be divisor of n such that $\frac{n}{m}$ is odd. Then there exist symmetric polynomials $R_{n,m}(\alpha, \beta)$ and $S_{n,m}(\alpha, \beta)$ with integral coefficients such that*

$$\phi(\alpha, \beta; n) = R_{n,m}^2(\alpha, \beta) - \left(\frac{-1}{m}\right) m\alpha\beta S_{n,m}^2(\alpha, \beta) (m \textit{ odd}) \tag{3}$$

$$\phi(\alpha, \beta; 2n) = \phi(\alpha, -\beta; n) = R_{n,m}^2(\alpha, -\beta) + \left(\frac{-1}{m}\right) m\alpha\beta S_{n,m}^2(\alpha, -\beta) (m \textit{ odd}) \tag{4}$$

Lemma 3 (Theorem of Meyer [9], see Dickson [5], p. 418, Narkiewicz [10], p. 72, Bachmann [1], pp. 272–307). *Among the primes represented by the irreducible primitive, positive or indefinite quadratic form $ax^2 + bxy + cy^2$, infinitely many are representable by any given linear form $Mn + N$ with M, N relatively prime, provided a, b, c, M, N are such that the linear and quadratic form can represent the same number.*

Lemma 4 (Rotkiewicz [11], Lemma 5). *Let $\psi(a) = 2a^2 \prod_{p|a}(p^2 - 1)$, where p runs over the prime factors of the positive integer a. If q is a prime such that $q^2 \| n$ and a is a natural number with $\psi(a) \mid q - 1$, then*

$$\phi(\alpha, \beta; n) \equiv 1 (\operatorname{mod} a),$$

where α, β are roots of the trinomial $x^2 - Px + Q$ and $(P, Q) = 1$.

Lemma 5 ([14]). *Let for a given discriminant d, $\overline{X}$ be the set of all generic characters. If for some integer e and some primitive quadratic form f with discriminant d we have $\chi(f) = \chi(e)$ for all $\chi \in \overline{X}$, then for every m prime to e the congruence*

$$f(x, y) \equiv e (\operatorname{mod} m),$$

where $f(x, y) = ax^2 + bxy + cy^2$, is solvable.

Proof of Theorem. By the assumptions of our Theorem we have $4D \mid A$, B is odd and $(D, d) = 1$.

Since arithmetic progression $AX + B$, where $(A, B) = 1$ contains an odd integer n_0 with $(D/n_0) = \varepsilon$, thus arithmetic progression $AX + B$, where $(A, B) = 1$, contains a prime number p such that

$$p \equiv n_0 (\operatorname{mod} 4D) \quad \text{and} \quad (D/n_0) = \varepsilon. \tag{5}$$

Let

$$2^\lambda \| B - (D/B) = B - (D/n_0) = B - \varepsilon, \quad \lambda \geq 1.$$

Now let p_1, p_2, p_3, p_4, p_5 be odd primes such that $(p_1 p_2 p_3 p_4 p_5, A\overline{\alpha\beta}d) = 1$ and q be a prime number such that

$$\psi\left(2^{\lambda+1} A p_1 p_2 p_3 p_4 p_5\right) \mid q - 1. \tag{6}$$

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

$$\begin{aligned} m &\equiv (D/n_0) + p_1 p_2 p_3 p_4 p_5 q^2 \overline{\alpha\beta} d \left(\operatorname{mod} p_1^2 p_2^2 p_3^2 p_4^2 p_5^2 q^3 \overline{\alpha\beta} d\right) \\ m &\equiv B \operatorname{mod} \left(2^{\lambda+1} A\right), \end{aligned} \tag{7}$$

where $B \equiv n_0 (\operatorname{mod} 4D)$.

Now we shall consider the congruence

$$ax^2 + bxy + cy^2 \equiv m \left(\operatorname{mod} 2^{\lambda+1} A p_1^2 p_2^2 p_3^2 p_4^2 p_5^2 q^3 \overline{\alpha\beta} d\right). \tag{8}$$

Since $m = (D/n_0) + p_1 p_2 p_3 p_4 p_5 q^2 \overline{\alpha\beta} d + l \cdot p_1^2 p_2^2 p_3^2 p_4^2 p_5^2 q^3 \overline{\alpha\beta} d$ and every prime factor $\overline{p_i}$ of d is of the form $4k + 1$ thus $\left(\frac{m}{\overline{p_i}}\right) = \left(\frac{\pm 1}{\overline{p_i}}\right) = 1$.

Since quadratic form $ax^2 + bxy + cy^2$ belongs to the principal genus, by Lemma 5 the congruence (8) has a solution in integers x and y.

Thus by Theorem of Meyer (Lemma 3) the quadratic form $ax^2 + bxy + cy^2$ represents infinitely many primes p of the arithmetic progression

$$2^{\lambda+1} A \overline{\alpha\beta} d q^3 p_1^2 p_2^2 p_3^2 p_4^2 p_5^2 z + m$$

$$\text{and} \quad p \equiv B (\operatorname{mod} A), (D/p) = (D/B) = (D/n_0) = \varepsilon.$$

Now our consideration rest on the fact that for each $\mu = \lambda$, $\lambda - 1$ at most one of the numbers $m_i = \phi\left(\alpha, \beta; \frac{p - (D/p)}{2^\mu p_i}\right)$ for $i = 1, 2, 3, 4, 5$ is divisible by p and at most

one is divisible by the highest prime factor r of $p - (D/p)$ (for the proof see [12], [13]).
Thus without loss of generality one can assume that neither $m_1 = \phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\mu p_1}\right)$ nor $m_2 = \phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\mu p_2}\right)$ nor $m_3 = \phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\mu p_3}\right)$ is divisible by p or r.

At least 2 of these numbers have the same sign. Thus without loss of generality one can assume that the numbers m_1 and m_2 have the same sign, hence $m_1 \cdot m_2 > 0$.

By Lemma 1 we can assume that

$$\left|\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\mu p_i}\right)\right| > 1 \text{ for } i = 1, 2.$$

Since $q^2 || \frac{p-(D/p)}{2^\mu p_1}$ and by (6), $\psi\left(2^{\lambda+1} A p_1 p_2 p_3 p_4 p_5\right) \mid q - 1$, we have by Lemma 4 that $m_1 \cdot m_2 \equiv 1 (\operatorname{mod} 4A)$. Since $\psi(4D) \mid q - 1$ and $q^2 || \frac{p-(D/p)}{p_1 p_2}$ by Lemma 4 we have $m_1 \cdot m_2 \equiv 1 (\operatorname{mod} 4D)$, hence $(D/m_1 m_2) = 1$ and $(D/p m_1 m_2) = (D/p) \cdot (D/m_1 m_2) = \varepsilon \cdot 1 = \varepsilon$.

We have (see [14], p. 417)

$$\begin{aligned} n = p\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\mu p_1}\right) \cdot \phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\mu p_2}\right) \left|U\left(\alpha, \beta; p - (D/p)\right)\right| \\ U\left(\alpha, \beta; p\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\mu p_1}\right)\right) \cdot \phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\mu p_2}\right) - (D/p) = \\ = U\left(\alpha, \beta; n - (D/p)\right) \end{aligned}$$

and n is a Lucas pseudoprime with parameters P and Q of the form $AX + B$ with $(D/n) = \varepsilon$.

Now we shall prove that our Lucas pseudoprimes for suitable μ are of the form $ax^2 + bxy + cy^2$.

We shall prove that $m_1 m_2 = \phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\mu p_1}\right) \phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\mu p_2}\right)$ is of the form $e^2 - dg^2$ for a suitable value of μ. Since $d > 0$ and d odd ($d \equiv 1 (\operatorname{mod} 4)$) it is enough to consider two cases.

First case: $|\overline{\alpha\beta}| \equiv \operatorname{sign}(\alpha\beta) (\operatorname{mod} 4)$.

We have $\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\lambda p_1}\right) = \phi\left(\alpha^u, \beta^u; dqw\right)$, where dqw is square-free and $\overline{\alpha\beta} \mid dqw, 2 \nmid u, 2 \nmid dqw$.

By Schinzel's formula (3) (Lemma 2) we have

$$\begin{aligned} \phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\lambda p_1}\right) = \phi\left(\alpha^u, \beta^u; dqw\right) = R^2_{dqw,\, d|\overline{\alpha\beta}|}\left(\alpha^u, \beta^u\right) - \\ - \left(\frac{-1}{d\left|\overline{\alpha\beta}\right|}\right) d\left|\overline{\alpha\beta}\right| (\alpha\beta)^u S^2_{dqw,\, d|\overline{\alpha\beta}|}\left(\alpha^u, \beta^u\right) = e^2 - dg^2, \end{aligned}$$

since $\left(\frac{-1}{d|\overline{\alpha\beta}|}\right) \left|\overline{\alpha\beta}\right| (\alpha\beta)^u$ is a square.

Since polynomials $R_{n,m}(\alpha, \beta)$ and $S_{n,m}(\alpha, \beta)$ are symmetric, the numbers

$$R^2_{dqw,\, d|\overline{\alpha\beta}|}\left(\alpha^u, \beta^u\right),\ S^2_{dqw,\, d|\overline{\alpha\beta}|}\left(\alpha^u, \beta^u\right)$$

are rationally expressible in terms of $\alpha^u + \beta^u$, $(\alpha\beta)^u$, hence they are rationally expressible by $\alpha + \beta = P$ and $\alpha\beta = Q$ and since they are algebraic integers and the numbers $\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\lambda p_1}\right)$, $\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\lambda p_2}\right)$ are of the form $e^2 - dg^2$.

¿From the identity

$$\left(ax^2 + bxy + cy^2\right)\left(z^2 - dt^2\right) = a(xz - bxt - 2cyt)^2 + \\ + b(xz - bxt - 2cyt)(2axt + byt + yz) + c(2axt + byt + yz)^2$$

we see that the number $n = p\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\lambda p_1}\right)\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^\lambda p_2}\right)$ is a Lucas pseudoprime with parameters P and Q of the form $ax^2 + bxy + cy^2$ and belongs to the arithmetic progression $AX + B$ with Jacobi symbol $(D/n) = \varepsilon$.

Second case: $\left|\overline{\alpha\beta}\right| \equiv -\operatorname{sign}(\alpha\beta) (\operatorname{mod} 4)$.

By Schinzel's formula (4) (Lemma 2) we have

$$\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^{\lambda-1}p_1}\right) = \phi\left(\alpha^u, -\beta^u; dqw\right) = R^2_{dqw,\, d\left|\overline{\alpha\beta}\right|}\left(\alpha^u, -\beta^u\right) + \\ + \left(\frac{-1}{d\left|\overline{\alpha\beta}\right|}\right) d\left|\overline{\alpha\beta}\right|(\alpha\beta)^u S^2_{dqw,\, d\left|\overline{\alpha\beta}\right|}\left(\alpha^u, -\beta^u\right) = e^2 - d\overline{g}^2,$$

since $-\left(\frac{-1}{d\left|\overline{\alpha\beta}\right|}\right)\left|\overline{\alpha\beta}\right|(\alpha\beta)^u$ is a square.

Similarly $\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^{\lambda-1}p_2}\right) = \bar{\bar{e}} - d\bar{\bar{e}}^2$, and the number $\overline{n} = p\phi\left(\alpha, \beta; \frac{p-(D/p)}{2^{\lambda-1}p_1}\right) \cdot \phi\left(\alpha, \beta; \frac{p-(D/p)}{2^{\lambda-1}p_2}\right)$ is a Lucas pseudoprime with parameters P and Q of the form $ax^2 + bxy + cy^2$ and belongs to the arithmetic progression $AX + B$ with the Jacobi symbol $(D/\overline{n}) = \varepsilon$.

References

[1] Bachmann, P., *Zahlentheorie. 2*, Die analytische Zahlentheorie, Tenbner, Leipzig, 1894.

[2] Baillie, R. & Wagstaff Jr., S., *Lucas pseudoprimes*, Math. Comp. 35 (1980), 1391–1417.

[3] Bilu Yu., Hanrot G. and Vouter P. M., *Existence of primitive divisors of Lucas and Lehmer numbers* (with an appendix by Mignott M.), J. Reine Angew. Math. 539 (2001), 75–122.

[4] Crandall, R. and Pomerance, C., *Prince Numbers*, A Computational Perspective, Springer-Verlag, New York, 2001.

[5] Dickson L. E., *History of the Theory of Numbers*, Vol. I, Chelsea Publishing Company, New York, 1952.

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

[7] Erdős, P., Kiss, P. and Sárközy, A., *Lower bound for the counting function*, Math. Comp. 51 (1988), 315–323.

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

[9] Meyer, A *Ueber einen Satz von Dirichlet*, J. reine angew. Math. 103 (1888), 98–117.

[10] Narkiewicz, W., *The Development of Prime Number Theory: from Euclid to Hardy and Littlewood*, Springer, 2000.

[11] Rotkiewicz, A., *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.

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

[13] ROTKIEWICZ, A., *On strong pseudoprimes in the case of negative discriminant in arithmetic progressions*, Acta Arith. 68 (1994), 145–151.

[14] ROTKIEWICZ, A., *On Lucas pseudoprimes of the form $ax^2 + bxy + cy^2$*, Applications of Fibonacci Numbers, Volume 6, Edited by G.E. Bergum, A.N. Philippou and A.F. Horadam, Kluwer Academic Publishers, Dordrecht, 1996, 409–421.

[15] ROTKIEWICZ, A. and A. SCHINZEL, *Sur les nombres pseudopremiers de la forme $ax^2 + bxy + cy^2$*, C.R. Acad. Sci. Paris, 258 (1964), 3617-3620.

[16] ROTKIEWICZ, A. and SCHINZEL, A., *On Lucas pseudoprimes with a prescribed value of the Jacobi symbol*, Bull. Polish Acad. Sci. Math. 48 (2000), 77–80.

[17] SCHINZEL, A., *On primitive prime factors of $a^n - b^n$*, Proc. Cambridge Philos. Soc. 58 (1962), 555–562.

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

[19] STEWART, C. L., *Primitive divisors of Lucas and Lehmer sequences*, Transcendence Theory: Advances and Applications (A. Baker and D.W. Masser, eds.), Academic Press, New York, 1977, pp. 79–92.

[20] WARD, M., *The intrinsic divisor of Lehmer numbers*, Ann. of Math. (2) 62 (1955), 230-236.

INSTITUTE OF MATHEMATICS, POLISH ACADEMY OF SCIENCES, UL. ŚNIADECKICH 8, SKR. POCZT. 137, 00-950 WARSZAWA, POLAND
E-mail address: rotkiewi@impan.gov.pl