ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria I: PRACE MATEMATYCZNE IX (1965)

A. SCHINZEL (Warszawa)

On the composite Lehmer numbers with prime indices, I

W. Sierpiński has recently deduced from a certain conjecture of the present writer (cf. [3], p. 188) the existence of infinitely many composite integers of the form $\frac{g^p-1}{g-1}$ (g any given integer >1, p prime) and also of the form $\frac{2^p+1}{3}$ (cf. [4] and [5]).

This suggests an analogous problem for $\frac{a^p-b^p}{a-b}$ (a, b integers) and more generally for the so-called *Lehmer numbers*

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

where α, β are roots of the trinomial $z^2-L^{1/2}z+M$ and L, M are rational integers.

The aim of this paper is to deduce from the aforesaid conjecture

H. *If $f_1, f_2, \ldots, f_k$ are irreducible polynomials with integral coefficients and the highest coefficients positive and such that $f_1(x)f_2(x)\ldots f_k(x)$ has no fixed factor greater than 1, then for infinitely many integers x, $f_i(x)$ $(i = 1, \ldots, k)$ are primes*;

the existence of infinitely many composite integers $P_p(\alpha, \beta)$ if α, β are rational $\neq 0$, $\alpha \neq \pm\beta$ or if α, β are irrational and some additional restrictions hold. Since the same method of proof gives some weaker but unconditional results we shall prove simultaneously the following two theorems.

THEOREM 1. *If $LM \neq 0$, $K = L-4M \neq 0$ and none of the numbers $-KL$, $-3KL$, $-KM$, $-3KM$ is a perfect square or each of the numbers K, L is a perfect square, then there exists an integer $k>0$ such that for every integer $D \neq 0$ one can find a prime q satisfying* [1]

$$q \mid P_{(q-(KL|q))/k} \quad \textit{and} \quad \left(\frac{1}{k}\big(q-(KL|q)\big), D\right) = 1.$$

[1] $(KL|q)$ is Jacobi's symbol of quadratic character.

Theorem 2. *Under the assumptions of Theorem* 1, *Conjecture* H *implies the existence of infinitely many primes* p *such that* $P_p(\alpha, \beta)$ *is composite.*

I think it very probable that Theorems 1 and 2 are true under the necessary assumption that α/β is not a root of unity, but the proof of that would require the use of reciprocity laws of degrees > 4. In our case we manage with the quadratic, cubic and biquadratic reciprocity laws only. We begin with two very elementary lemmas.

Lemma 1. *If* a, b *are two square-free integers, such that* $b \neq -1, -3$ *and* $ab \pm -d^2, -3d^2$ *then there exists an odd integer* $m > 0$ *such that*

$$(1) \qquad (a\,|\,m) = 1 \quad \textit{and} \quad \left(\tfrac{1}{2}\big(m-(b\,|\,m)\big),\ 2ab\right) = 1.$$

Proof. Let us remark that for every odd square-free modulus $\mu \neq \pm 1, \pm 3$, there exists an integer ν such that $(\nu+1, \mu) = 1$ and $(\nu\,|\,\mu) = -1$. In fact, such a $\nu = \nu(\mu)$ clearly exists if $|\mu|$ is a prime. If μ is not a prime, and q is its greatest prime factor, it suffices to take

$$\nu(\mu) \equiv \begin{cases} \nu(q) \bmod q, \\ 1 \bmod \mu/q. \end{cases}$$

Now, put $a = da_1$, $b = db_1$, where $(a_1, b_1) = 1$ and $b_1 > 0$. Since a, b are square-free, we have $(da_1, b_1) = 1$. We notice that if $b_1 = 1$ or 3, then $a_1 \neq -1, -3$ and $d \neq -1, -3$. We shall define m by a system of congruences different for each of the following 7 cases.

1. b_1 even:

$$m \equiv \begin{cases} 1 \bmod da_1b_1, \\ 5 \bmod 8. \end{cases}$$

2. b_1 odd $\neq 1, 3$:

$$m \equiv \begin{cases} 1 \bmod 4da_1, \\ \nu(b_1) \bmod b_1. \end{cases}$$

3. $b_1 = 1$ or 3, $a_1 > 0$, $d > 0$:

$$m \equiv -1 \bmod 4da_1b_1.$$

4. $b_1 = 1$ or 3, $da_1 < 0$ and $\min(a_1, d)$ is even:

$$m \equiv \begin{cases} -1 \bmod da_1b_1, \\ 3 \bmod 8. \end{cases}$$

5. $b_1 = 1$ or 3, $da_1 < 0$ and $\min(a_1, d)$ is odd:

$$m \equiv \begin{cases} -1 \bmod 8b_1 \max(a_1, d), \\ -\nu\big(\min(a_1, d)\big) \bmod \min(a_1, d). \end{cases}$$

6. $b_1 = 1$ or 3, $a_1 < 0$, $d < 0$ and da_1 is even:

$$m \equiv \begin{cases} 1 \bmod b_1 \times \mathrm{even}\,(a_1, d) \\ \nu\big(\mathrm{odd}(a_1, d)\big) \bmod \mathrm{odd}(a_1, d), \\ 5 \bmod 8, \end{cases}$$

where even (a_1, d) and odd(a_1, d) denote the even and the odd one of the numbers a_1 and d.

7. $b_1 = 1$ or 3, a_1 and d are odd < 0:

$$m \equiv \begin{cases} 1 \bmod 4b_1, \\ \nu(a_1) \bmod a_1, \\ \nu(d) \bmod d. \end{cases}$$

It follows from the Chinese Remainder Theorem that the above systems of congruences are solvable and from the quadratic reciprocity law that any of their positive solutions satisfies (1).

LEMMA 2. *If γ is any integer > 0 and c any square-free integer, then there exists an odd integer $m > 0$ such that*[2]

$$(2) \qquad 2^\gamma \| m-1, \qquad (c|m) = -1 \qquad \textit{and} \qquad (m-1, c) = (2, c)$$

except for

$$\gamma = \begin{cases} 1 \ \textit{if} \ c = 1 \ \textit{or} \ 3, \\ 2 \ \textit{if} \ c = \pm 1 \ \textit{or} \ \pm 6, \end{cases}$$
$$\gamma \geqslant 3 \ \textit{if} \ c = \pm 1 \ \textit{or} \ \pm 2.$$

Proof. For $\gamma = 1$, we put in Lemma 1: $a = -c$, $b = 1$. If $c \neq 1, 3$, the conditions of that lemma are satisfied and there exists an odd integer $m > 0$ such that

$$(-c|m) = 1, \qquad \big(\tfrac{1}{2}(m-1), 2c\big) = 1.$$

Hence $m \equiv 3 \bmod 4$, $(c|m) = -1$ and $(m-1, c) = (2, c)$; so in this case conditions (2) are satisfied.

For $\gamma \geqslant 2$ we define m by a system of congruences different for each of the following cases.

1. $|c| \equiv 3 \bmod 4$ or $|c| \equiv 2 \bmod 8$, $\gamma = 2$ or $|c| \equiv 6 \bmod 8$, $\gamma \geqslant 3$:

$$m \equiv \begin{cases} -1 \bmod c, \\ 2^\gamma + 1 \bmod 2^{\gamma+1}. \end{cases}$$

2. $|c| \equiv 1 \bmod 4$, $c \neq \pm 1$:

$$m \equiv \begin{cases} -\nu(c) \bmod c, \\ 2^\gamma + 1 \bmod 2^{\gamma+1}. \end{cases}$$

[2] $2^\gamma \| m-1$ means that $2^\gamma | m-1$ and $2^{\gamma+1} \nmid m-1$.

3. $|c| \equiv 6 \bmod 8$, $\gamma = 2$, $c \neq \pm 6$ or $|c| \equiv 2 \bmod 8$, $\gamma \geqslant 3$, $c \neq \pm 2$:

$$m \equiv \begin{cases} -\nu(c/2) \bmod c, \\ 2^{\gamma}+1 \bmod 2^{\gamma+1}. \end{cases}$$

It follows from the Chinese Remainder Theorem that the above systems of congruences are solvable and from the quadratic reciprocity law that any of their positive solutions satisfies (2).

Proof of Theorems 1 and 2. In the course of this proof we can assume without loss of generality that $(L, M) = 1$, i.e. $(\alpha, \beta) = 1$. We shall denote by $k(n)$ the square-free kernel of any given integer $n \neq 0$. Suppose first that none of the numbers $-KL$, $-3KL$, $-KM$, $-3KM$ is a perfect square. Then it suffices to take $k = 2$. In fact, by Lemma 1 there exists an odd integer $m > 0$ such that

$$\big(k(LM)\,|\,m\big) = 1 \quad \text{and} \quad \Big(\tfrac{1}{2}\big(m - \big(k(KL)\,|\,m\big)\big), 2k(KL)k(LM)\Big) = 1.$$

Let us put

$$f_1(x) = 4k(KL)k(LM)x + m, \quad f_2(x) = \tfrac{1}{2}f_1(x) - \tfrac{1}{2}\big(k(KL)\,|\,m\big).$$

It is clear that the polynomial $f_1(x)f_2(x)$ has no fixed factor > 1. Further, if $f_1(x) = q$ is a prime, and $q \nmid KLM$, we have

$$(LM\,|\,q) = \big(k(LM)\,|\,m\big) = 1 \quad \text{and} \quad (KL\,|\,q) = \big(k(KL)\,|\,m\big),$$

because $(LM\,|\,r)$ and $(KL\,|\,r)$ considered for $r > 0$ are characters with conductors dividing $4KLM$. Hence by the formula (cf. [2], p. 223)

$$(\alpha/\beta)^{q/2-(KL|q)/2} \equiv (LM\,|\,q) \bmod q,$$

we find

$$q\,|\,P_{q/2-(KL|q)/2}(\alpha, \beta). \tag{3}$$

Now the theorems follow easily. First, for every $D \neq 0$ there exists an integer x_0 such that $\big(f_1(x_0)f_2(x_0), 4KLMD\big) = 1$. By Dirichlet's theorem there exists a prime

$$q = f_1(x) \equiv f_1(x_0) \bmod 4KLMD.$$

The prime q satisfies (3) and besides

$$\tfrac{1}{2}q - \tfrac{1}{2}(KL\,|\,q) \equiv f_2(x_0) \bmod D, \quad \big(\tfrac{1}{2}q - \tfrac{1}{2}(KL\,|\,q), D\big) = 1,$$

which proves Theorem 1 in this case. As to Theorem 2, Conjecture H implies the existence of infinitely many integers x such that $f_1(x) = q$ and $f_2(x) = p$ are both primes. Taking x so large that $q \nmid KLM$ we have by (3)

$$q\,|\,P_p(\alpha, \beta). \tag{4}$$

On the other hand, we have for $K > 0$

$$(5)\qquad |P_p(\alpha,\beta)| \geqslant \big(\max(|\alpha|,|\beta|)\big)^{p-2}(\alpha+\beta) \geqslant \left(\frac{1}{2}L^{1/2}+\frac{1}{2}K^{1/2}\right)^{p-2} \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{p-2}$$

and for $K < 0$, $p > N(\alpha,\beta)$ by the fundamental lemma of [1]:

$$(5')\qquad |P_p(\alpha,\beta)| \geqslant |\alpha|^{p-\log^3 p} \geqslant (\sqrt{2})^{p-\log^3 p}.$$

Thus for p large enough, $|P_p(\alpha,\beta)| > 2p+1 = q$ and (4) implies that $P_p(\alpha,\beta)$ is composite.

It remains to consider the case where K, L and one of the numbers $-KM$, $-3KM$ is a perfect square. In this case the numbers α and β are rational integers. For every pair L, M in question we shall give the value of k and construct two polynomials $f_1(x,y), f_2(x,y) = \frac{1}{k}\big(f_1(x,y)-1\big)$ of degree $d \leqslant 2$ satisfying the following conditions:

(i) polynomials $f_1(x,y), f_2(x,y)$ have integral coefficients, are primitive, irreducible as polynomials in x for every integral value of y and

$$(6)\qquad \big(f_1(0,0)f_2(0,0),(2d)!\big) = 1,$$

(ii) if $\big(f_1(x_0,y_0),\mu\big) = 1$, there exist infinitely many primes of the form $f_1(x,y) \equiv f_1(x_0,y_0) \bmod \mu$,

(iii) if $q = f_1(x,y)$ is a prime $\nmid M$, then

$$(7)\qquad q \mid (\alpha/\beta)^{(q-1)/k}-1.$$

These conditions being satisfied, Theorems 1 and 2 follow easily. First, by condition (i) and Gauss' Lemma the polynomial $f_1(x,y)f_2(x,y)$ is primitive of degree $2d$. Formula (6) implies that it has no fixed factor >1. Thus for every $D \neq 0$, there exist integers x_0, y_0 such that

$$(8)\qquad \big(f_1(x_0,y_0)f_2(x_0,y_0), kKLMD\big) = 1.$$

Now by condition (ii) there exist infinitely many primes of the form $f_1(x,y) \equiv f_1(x_0,y_0) \bmod kKLMD$.

For every such prime we have by (iii) divisibility (7); thus

$$(9)\qquad q \mid P_{(q-1)/k}(\alpha,\beta)$$

because $q \nmid KL$.

On the other hand,

$$\frac{q-1}{k} \equiv \frac{1}{k}\big(f_1(x_0,y_0)-1\big) \equiv f_2(x_0,y_0) \bmod D;$$

thus in view of (8), $\left(\frac{q-1}{k}, D\right) = 1$.

Further, (i) implies the existence of an integer y_0 such that $f_1(x, y_0)f_2(x, y_0)$ has no fixed factor >1. Since again by (i) the polynomials $f_1(x, y_0)$ and $f_2(x, y_0)$ are irreducible, Conjecture H implies that for infinitely many integers x, $q = f_1(x, y_0)$ and $p = f_2(x, y_0)$ are both primes. If we take x so large that

$$q \nmid KLM \quad \text{and} \quad \left(\frac{1+\sqrt{5}}{2}\right)^{p-2} > kp+1,$$

we have (9) and since $\frac{q-1}{k} = p$, the number $P_p(\alpha, \beta)$ is composite.

We now proceed to the construction of polynomial $f_1(x, y)$ and denote by N the greatest odd factor of M.

If $-3M$ is a perfect square, we put

$$k = 6, \quad f_1(x, y) = 4(3Nx+1)^2+27N^2(2y+1)^2.$$

Condition (i) is satisfied trivially. Further, if $(f_1(x_0, y_0), \mu) = 1$, then by Dirichlet's theorem for the field $K(\sqrt{-3})$, there exist infinitely many primes Q of that field satisfying the congruence

$$Q \equiv 6Nx_0+2+3N(2y_0+1)\sqrt{-3} \bmod 12N\mu.$$

A norm of any such prime Q is a rational prime q of the form $f_1(x, y)$ and satisfies the congruence $q \equiv f_1(x_0, y_0) \bmod \mu$. Condition (ii) is satisfied. As to (iii), we notice that $f_1(x, y) \equiv 1 \bmod 6$ and $(f_1(x, y), M) = 1$; thus if $q = f_1(x, y)$ is a prime, we get

$$(10) \qquad (\alpha\beta)^{(q-1)/2} \equiv (M|q) = (-3M|q)(-3|q) \equiv 1 \bmod q.$$

Further, it follows from the cubic reciprocity law that α and β are both cubic residues $\bmod q$; thus

$$(11) \qquad (\alpha/\beta)^{(q-1)/3} \equiv 1 \bmod q.$$

It follows from (10) and (11) that $(\alpha/\beta)^{(q-1)/6} \equiv 1 \bmod q$, i.e. condition (iii) is satisfied.

If $-M$ a perfect square, we put

$$(12) \qquad -M = e^{2^{\gamma-1}},$$

where γ is an integer $\geqslant 2$ and e is a positive integer not being a perfect square (this is possible since $-M \neq 0, 1$).

If neither $\gamma = 2$, $e = 6f^2$ nor $\gamma \geqslant 3$, $e = 2f^2$, then by Lemma 2 there exists an odd integer $m > 0$ such that

$$(13) \qquad 2^\gamma \| m-1, \quad (k(e)|m) = -1, \quad (m-1, k(e)) = (2, k(e)).$$

We put

$$k = 2^\gamma, \quad f_1(x, y) = f_1(x) = 2^{\gamma+1}k(e)x+m.$$

Condition (i) is satisfied trivially. Further if $(f_1(x_0), \mu) = 1$, then by Dirichlet's theorem there exist infinitely many primes

$$q \equiv f_1(x_0) \bmod 2^{\gamma+1} k(e)\mu .$$

These primes are clearly of the form $f_1(x)$, and thus condition (ii) is satisfied. As to (iii), if $q = f_1(x) > 0$ and $(q, e) = 1$, we have by (13)

$$2^\gamma \| q-1, \quad (e|q) = -1,$$

since $(e|r)$ considered for $r > 0$ is a character with conductor dividing $4k(e)$. Hence if q is a prime $\nmid M$, we get

$$(14)\quad M^{(q-1)/2^\gamma} \equiv (-1)^{(q-1)/2^\gamma}(e^{2^{\gamma-1}})^{(q-1)/2^\gamma} \equiv -e^{(q-1)/2} \equiv -(e|q) \equiv 1 \bmod q.$$

On the other hand, it follows from (12), $\alpha\beta = M$ and $(\alpha, \beta) = 1$ that

$$(\alpha^2)^{(q-1)/2^\gamma} \equiv (\beta^2)^{(q-1)/2^\gamma} \equiv 1 \bmod q;$$

thus by (14)

$$(\alpha/\beta)^{(q-1)/2^\gamma} \equiv M^{(q-1)/2^\gamma} \equiv 1 \bmod q,$$

which proves condition (iii).

If $\gamma = 2$, $e = 6f^2$, we put

$$k = 12, \quad f_1(x, y) = (6Nx + 3N + 2)^2 + 108N^2(2y+1)^2 .$$

Condition (i) is satisfied trivially. Further, if $(f_1(x_0, y_0), \mu) = 1$, then by Dirichlet's theorem for the field $K(\sqrt{-3})$ there exist infinitely many primes Q of this field satisfying the congruence

$$Q \equiv 6Nx_0 + 3N + 2 + 6N(2y_0+1)\sqrt{-3} \bmod 24N\mu .$$

A norm of any such prime Q is a rational prime q of the form $f_1(x, y)$ and satisfies the congruence $q \equiv f_1(x_0, y_0) \bmod \mu$. Condition (ii) is satisfied. As to (iii), if $q = f_1(x, y)$ is a prime $\nmid M$, then by the cubic reciprocity law α and β are both cubic residues $\bmod q$, and thus

$$(15)\qquad (\alpha/\beta)^{(q-1)/3} \equiv 1 \bmod q.$$

Further, since $\alpha\beta = M = -36f^4$ and $(\alpha, \beta) = 1$, each of the numbers $|\alpha|$ and $|\beta|$ is a perfect square and we get

$$(\alpha/\beta)^{(q-1)/4} \equiv M^{(q-1)/4} \equiv (-1)^{(q-1)/4} 6^{(q-1)/2} \bmod q.$$

However, $q \equiv 13 \bmod 24$, and thus

$$(16)\qquad (\alpha/\beta)^{(q-1)/4} \equiv -6^{(q-1)/2} \equiv -(6|q) \equiv 1 \bmod q.$$

It follows from (15) and (16) that $(\alpha/\beta)^{(q-1)/12} \equiv 1 \bmod q$, i.e. condition (iii) is satisfied.

If $\gamma \geqslant 3$, $e = 2f^2$ we put $e = 2^{\delta}g^2$, g odd.

By the Chinese Remainder Theorem the systems of congruences

$$u^2 \equiv \begin{cases} 4 \bmod k(g), \\ 2^{\gamma+1}+1 \bmod 2^{\gamma+2}, \end{cases} \qquad v^2 \equiv \begin{cases} 4 \bmod 3k(g), \\ 2^{\gamma+1}+1-16k(g)^2 \bmod 2^{\gamma+2} \end{cases}$$

are solvable for every $\gamma \geqslant 3$. Denote by u_γ, v_γ any of their solutions and put $k = 2^{\gamma+1}$,

$$f_1(x, y) = \begin{cases} \big(2^{\gamma+1}k(g)x + u_\gamma\big)^2 + 2^{2\gamma}\big(k(g)/3\big)^2(3y+1)^2, & \text{if } 3 \mid k(g), \\ \big(3\cdot 2^{\gamma+1}k(g)x + v_\gamma\big)^2 + k(g)^2(3\cdot 2^\gamma y + 4)^2, & \text{if } 3 \nmid k(g). \end{cases}$$

Condition (i) is satisfied in view of the choice of u_γ, v_γ. Further, if $\big(f_1(x_0, y_0), \mu\big) = 1$, then by Dirichlet's theorem for the field $K(i)$ there exist infinitely many primes Q of that field satisfying the congruence

$$Q \equiv \begin{cases} 2^{\gamma+1}k(g)x_0 + u_\gamma + 2^\gamma \dfrac{k(g)}{3}(3y_0+1)i \bmod 2^{\gamma+1}k(g), & \text{if } 3 \mid k(g), \\ 3\cdot 2^{\gamma+1}k(g)x_0 + v_\gamma + k(g)(3\cdot 2^\gamma y_0 + 4)i \bmod 3\cdot 2^{\gamma+1}k(g), & \text{if } 3 \nmid k(g). \end{cases}$$

A norm of any such prime Q is a rational prime q of the form $f_1(x, y)$ and satisfies the congruence $q \equiv f_1(x_0, y_0) \bmod \mu$. Condition (ii) is, therefore, satisfied. As to (iii), we consider the cases $3 \mid k(g)$ and $3 \nmid k(g)$ separately.

If $3 \mid k(g)$ and q is a prime of the form $f_1(x, y)$, then by the biquadratic reciprocity law, 2 and $k(g)/3$ are both biquadratic residues $\bmod q$; thus $2^\delta g^2/9 = e/9$ is also such a residue. If $q \nmid M$ we have, since $q \equiv 5 \bmod 12$,

$$e^{(q-1)/4} \equiv (e/9)^{(q-1)/4} 9^{(q-1)/4} \equiv 3^{(q-1)/2} \equiv (3 \mid q) \equiv -1 \bmod q.$$

Since $(q-1)/2^{\gamma+1}$ is odd, we get

$$M^{(q-1)/2^{\gamma+1}} \equiv (-1)^{(q-1)/2^{\gamma+1}} \big(e^{2^{\gamma-1}}\big)^{(q-1)/2^{\gamma+1}} \equiv -e^{(q-1)/4} \equiv 1 \bmod q.$$

Further, since $\alpha\beta = M = -4f^{2^\gamma}$ and $(\alpha, \beta) = 1$, one of the numbers α^2, β^2 must be a perfect $2^{\gamma+1}$-th power; thus

$$(\alpha/\beta)^{(q-1)/2^{\gamma+1}} \equiv M^{(q-1)/2^{\gamma+1}} \equiv 1 \bmod q,$$

which proves condition (iii).

If $3 \nmid k(g)$ and q is a prime of the form $f_1(x, y)$, then by the biquadratic reciprocity law, $k(g)$ is a biquadratic residue $\bmod q$ but 2 is not. If $q \nmid M$, this gives

$$e^{(q-1)/4} \equiv \big(2^{(q-1)/4}\big)^\delta g^{(q-1)/2} \equiv -1 \bmod q,$$

whence condition (iii) follows as before. This completes the proof.

References

[1] A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ak. Mat. 4 (1962), pp. 413-416.

[2] — *On primitive prime factors of Lehmer numbers I*, Acta Arith. 8 (1963), pp. 213-223.

[3] — et W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), pp. 185-208.

[4] W. Sierpiński, *Sur les nombres premiers dont tous les chiffres sont egaux à* 1, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fiz. Mat. Nat. 31 (1961), pp. 347-349.

[5] — *O liczbach złożonych postaci* $(2^p+1)/3$, *gdzie* p *jest liczbą pierwszą*, Prace Mat. 7 (1962), pp. 169-172.