Reprinted from *The Journal of Mathematical Sciences*
Vol. 1 No. 1 (January, 1966)

A REMARK ON RECURSIVE SEQUENCES

K. MAHLER

A REMARK ON RECURSIVE SEQUENCES

K. MAHLER

[Received 19 November, 1965]

1. Let

$$f(x) = x^2 + ax + b$$

be a polynomial with integral coefficients satisfying

$$d = 4b - a^2 > 0, \qquad (a, b) = 1. \tag{1}$$

The zeros

$$\alpha = \tfrac{1}{2}(-a + \sqrt{-d}), \qquad \alpha' = \tfrac{1}{2}(-a - \sqrt{-d})$$

of $f(x)$ are thus conjugate complex numbers, and they are conjugate algebraic numbers in the imaginary quadratic field $K = R(\sqrt{-d})$ generated by $\sqrt{-d}$.

With $f(x)$ is associated the linear difference equation

$$w_{n+2} + aw_{n+1} + bw_n = 0, \tag{2}$$

where n is assumed to run over the positive integers. We consider only solutions w_n that are integral for all such n and do not vanish identically.

I shall in this note establish a lower bound for $| w_n |$ which, except in certain trivial cases, tends rapidly to infinity with n.

2. The two special solutions

$$u_n = \frac{\alpha^n - \alpha'^n}{\alpha - \alpha}, \quad v_n = \alpha^n + \alpha'^n \tag{3}$$

of (2) are integral for all n and begin with the terms

$$u_1 = 1, u_2 = -a; \qquad v_1 = -a, v_2 = a^2 - 2b,$$

where

$$u_1 v_2 - u_2 v_1 = -2b \neq 0.$$

Hence there are three integers p, q, and $r > 0$, such that the sum

$$pu_n + qv_n - rw_n, = z_n \text{ say,}$$

vanishes for $n = 1$ and $n = 2$. But z_n is a solution of (2), hence vanishes identically, and so it follows that

$$rw_n = pu_n + qv_n \text{ for all } n. \tag{4}$$

3. From

$$| \alpha | = | \alpha' | = + b^{1/2}$$

it is obvious that, as n tends to infinity,

$$\max(|u_n|, |v_n|, |w_n|) = O(b^{n/2}).$$

Here $b^{n/2}$ is bounded for all n only if $b = 1$. From now on let this trivial case be excluded; by (1), it occurs only for the three polynomials

$$x^2 + 1, \quad x^2 - x + 1, \quad \text{or} \quad x^2 + x + 1. \tag{5}$$

Then, from (3), also

$$\max(|u_n|, |v_n|) \geqslant c_0 b^{n/2}, \tag{6}$$

where c_0 denotes a positive constant that does not depend on n.

Put

$$\delta_n = (u_n, v_n).$$

We assert that δ_n may assume only the two values

1 and 2.

For let s be either 4 or an odd prime, and assume that, for some value of n, δ_n is divisible by s. Since

$$\alpha^n = \frac{v_n + u_n\sqrt{-d}}{2} \quad \text{and} \quad \alpha'^n = \frac{v_n - u_n\sqrt{-d}}{2}, \tag{7}$$

it follows that

$$\frac{2\alpha^n}{s} \quad \text{and} \quad \frac{2\alpha'^n}{s}$$

are integers in K. Denote by $\mathfrak{P}$ a prime ideal factor of s in K. Then evidently both α and α' are divisible by $\mathfrak{P}$, hence also

$$a = -(\alpha + \alpha') \quad \text{and} \quad b = \alpha\alpha'.$$

This implies that both a and b are divisible by 2 if $s = 4$, and by s otherwise, contrary to the hypothesis (1).

From now on put

$$x_n = \frac{u_n}{\delta_n} \quad \text{and} \quad y_n = \frac{v_n}{\delta_n}. \tag{8}$$

Both x_n and y_n are integers, and they are relatively prime; further, by (6), there exists a positive constant c_1 independent of n such that always

$$\max(|x_n|, |y_n|) \geqslant c_1 b^{n/2}. \tag{9}$$

From (3) it follows immediately that

$$du_n^2 + v_n^2 = 4b^n.$$

Hence

$$dx_n^2 + y_n^2 = \varepsilon_n b^n, \tag{10}$$

where

$$\varepsilon_n = 4/\delta_n^2$$

is either 1 or 4.

4. The equation

$$w_n = 0$$

is equivalent to $pu_n + qv_n = 0$, thus by (7) implies that

$$\left(\frac{\alpha}{\alpha'}\right)^n = \frac{p - q\sqrt{-d}}{p + q\sqrt{-d}}.$$

In general this condition for n has at most one solution; and by

$$\alpha \neq \alpha'$$

it cannot have more than one solution n unless α/α' is a root of unity distinct from -1. This root of unity lies in the imaginary quadratic field K and hence is one of the numbers

$$-1, \mp i, \quad \text{or} \quad \frac{\mp 1 \mp \sqrt{-3}}{2}.$$

Now

$$\frac{\alpha}{\alpha'} = \frac{-a + \sqrt{-d}}{-a - \sqrt{-d}} = \frac{(a^2 - 2b) - a\sqrt{-d}}{2b}.$$

Therefore $\alpha/\alpha' = -1$ demands that $a = 0$, hence by (1) that $b = 1$; and so

$$f(x) = x^2 + 1,$$

a case already excluded. Similarly $\alpha/\alpha' = \mp i$ requires that $a^2 - 2b = 0$, which is impossible by (1). Finally

$$\frac{\alpha}{\alpha'} = \frac{\mp 1 \mp \sqrt{-3}}{2} \text{ can hold only if } \frac{a^2 - 2b}{2b} = \mp \frac{1}{2},$$

thus if either $a^2 = b$ or $a^2 = 3b$. The second case is again excluded by (1); the first case holds for $a = \mp 1$, $b = 1$, hence for

$$f(x) = x^2 - x + 1 \quad \text{and} \quad f(x) = x^2 + x + 1,$$

and these two cases have also been excluded.

We have then the result that if $f(x)$ is not one of the three polynomials (5), then at most one term of the recursive sequence w_n can vanish.

5. From now on let then n already be so large that

$$w_n \neq 0. \tag{11}$$

We can then study w_n by means of the p-adic generalisation of Roth's theorem due to *D. Ridout* [1]. We need one special case of this result which can be formulated as follows.

Let $F(x, y)$ be a binary cubic form with integral coefficients and of non-zero discriminant, and let x, y be any pair of integers satisfying

$$F(x, y) \neq 0, \qquad (x, y) = 1.$$

Let $p_1, p_2, \ldots, p_t$ be finitely many distinct primes, and let $P(x, y)$ denote the largest divisor of $F(x, y)$ that has at most these prime factors. Then, to every given constant $\varepsilon > 0$, there exists a positive number c independent of x and y such that

$$\frac{|F(x, y)|}{P(x, y)} \geqslant c \max(|x|, |y|)^{1-\varepsilon}.$$

This theorem will now be applied with

$$F(x, y) = (dx^2+y^2)(px+qy) \text{ and } x = x_n, \; y = y_n,$$

where the suffix n is assumed to be already sufficiently large so that (11) is satisfied. Obviously all three linear factors $F(x, y)$ are distinct so that its discriminant does not vanish. From (4) and (10),

$$F(x_n, y_n) = \delta_n^{-1} \varepsilon_n b^n r w_n \neq 0,$$

where naturally the right-hand side is an integer. Thus Ridout's theorem may be applied. For this purpose choose the set of primes $p_1, \ldots, p_t$ already so large that it contains in particular the prime 2 and all the prime factors of both b and r. In analogy to $P(x, y)$, let W_n be the largest divisor of w_n that has at most the prime factors $p_1, p_2, \ldots$ p_t. Since evidently

$$\frac{|F(x_n, y_n)|}{P(x_n, y_n)} = \frac{|w_n|}{W_n},$$

Ridout's theorem and the inequality (9) together imply that

$$\frac{|w_n|}{W_n} \geqslant c \max(|x_n|, |y_n|)^{1-\varepsilon} \geqslant c_2 b^{\frac{1}{2}(1-\varepsilon)n}, \tag{12}$$

where the new constant

$$c_2 = c\, c_1^{1-\varepsilon} > 0$$

is independent of n.

If in (12) we decrease the number of primes $p_1, p_2, \ldots, p_t$, W_n cannot increase, but may decrease, and so this inequality is still valid. We arrive thus finally at a result which may be formulated as follows.

Theorem: Let a and b be integers satisfying

$$4b > a^2, \qquad b \geqslant 2, \qquad (a, b) = 1.$$

Denote by $w_1, w_2, w_3, \ldots$ a sequence of integers not all zero such that

$$w_{n+2} + aw_{n+1} + bw_n = 0 \quad \textit{for} \quad n = 1, 2, 3, \ldots .$$

Let $p_1, p_2, \ldots, p_t$ be finitely many distinct primes, and let W_n be the largest divisor of w_n that has at most these prime divisors. Let finally $\varepsilon > 0$ be an *arbitrary constant. Then, as soon as n is sufficiently large,*

$$\frac{|w_n|}{W_n} \geqslant b^{\left(\frac{1}{2}-\varepsilon\right)n} \quad \textit{and hence also} \quad |w_n| \geqslant b^{\left(\frac{1}{2}-\varepsilon\right)n}.$$

For we have

$$c_2 b^{\frac{1}{2}(1-\varepsilon)n} = b^{\left(\frac{1}{2}-\varepsilon\right)n} \cdot c_2 b^{\frac{1}{2}\varepsilon n} \geqslant b^{\left(\frac{1}{2}-\varepsilon\right)n} \text{ as soon as } c_2 b^{\frac{1}{3}\varepsilon n} \geqslant 1.$$

This theorem is nearly best possible because

$$w_n = O(b^{n/2}).$$

There is an analogous theorem for the case when $4b < a^2$ which can be proved in the same way.

One of the consequences of the theorem deserves to be mentioned.

COROLLARY. *Under the hypothesis of the theorem, the greatest prime divisor of w_n tends to infinity with n.*

By way of example, the difference equation

$$w_{n+2} - w_{n+1} + 2w_n = 0$$

is satisfied by the sequence

$$0, 1, 1, -1, -3, -1, 5, 7, -3, -17, -11, 23, 45, -1, \ldots \text{ etc.}$$

which has a great number of terms ∓ 1; but we naturally are now certain that there are only finitely many such terms.

It would have much interest to extend the theorem to linear difference equations of higher order, but this will probably be difficult. In a previous paper [2], I proved a result of which a special case may be formulated as follows.

Let

$$f(x) = x^k + a_1 x^{k-1} + a_2 x^{k-2} + \ldots + a_k,$$

where $k \geqslant 2$, be a polynomial with integral coefficients and with the zeros $\alpha_1, \alpha_2, \ldots, \alpha_k$. Assume that the zero α_k is not a root of unity, and that none of the quotients $\frac{\alpha_1}{\alpha_k}, \frac{\alpha_2}{\alpha_k}, \ldots, \frac{\alpha_{k-1}}{\alpha_k}$ is a root of unity different from $+1$. If $w_1, w_2, w_3, \ldots$ is a sequence of integers not all zero that satisfy the difference equation

$$w_{k+n} + a_1 w_{k+n-1} + a_2 w_{k+n-2} + \ldots + a_k w_n = 0 \text{ for all } n,$$

then

$$\lim_{n \to \infty} |w_n| = \infty.$$

The proof of this theorem was based on a method due to Th. Skolem.

This result is much weaker than the theorem that we proved in the special case when $n = 2$.

The corollary is not new; see my note [3].

REFERENCES

1. D. RIDOUT. *Mathematika*, **5** (1958), 40-48.
2. K. MAHLER. *Proc. Kon. Akad. Wet. Amsterdam*, **38** (1935), 51-60.
3. K. MAHLER. *Mathematica B (Zutphen)*, **3** (1934-35), 1-4.

Mathematics Department, IAS,
Australian National University,
Canberra, ACT.