ARITHMETICAL PROPERTIES OF THE TAYLORCOEFFICIENTS OF ALGEBRAIC FUNCTIONS

BY

J. POPKEN

(Communicated at the meeting of April 25, 1959)

1. INTRODUCTION. Eisenstein's well-known theorem reads:

"Let the power series

$$\sum_{n=0}^{\infty} a_n z^n$$

with rational coefficients a_n, convergent in the neighbourhood of the origin, represent a branch of an algebraic function. If the $a_n = s_n/t_n$ are in their reduced forms, then the denominators t_n $(n = 0, 1, 2, \ldots)$ have at most a finite number of prime divisors." More general: "There exists a positive integer N such that all numbers $N^n a_n$ $(n = 1, 2, \ldots)$ are integers." Compare e.g. PÓLYA and SZEGÖ [6], p. 139.

Eisenstein's theorem does not give us any information about the arithmetical properties of the *nominators* s_n. This is a much deeper problem and, as far as I know, there are only very few results in this direction. PÓLYA [7] studied in 1915 the Taylor series with rational coefficients of a rational function with the property that all its non-vanishing coefficients have only a finite number of prime divisors in the nominators. He showed a.o. in which manner all such expansions can be derived from

$$\frac{1}{1-z} = 1 + z + z^2 + \ldots .$$

For another contribution to this problem, also for rational functions, see SIEGEL [9], Satz 8, p. 207.

In this paper I first prove some theorems which are closely connected with the problem stated above. The first three theorems have the following joint conditions:

Let the power series

$$f(z) = \sum_{n=0}^{\infty} a_n z^n,$$

with rational coefficients a_n and convergent in a neighbourhood $|z| < R$ of the origin, represent a branch of an algebraic function. We exclude the case that $f(z)$ represents a polynomial. Let b denote a rational number such that $0 < |b| < R$.

In the next three theorems we consider the corresponding partial sums

$$S_n = \sum_{\nu=0}^{n} a_\nu b^\nu \qquad (n = 0, 1, \ldots).$$

These are rational numbers and from Eisenstein's theorem it is clear that in their reduced forms the S_n have at most a finite number of prime divisors in their denominators. The following results show that the nominators of the S_n behave in quite a different way. We always write the S_n in their reduced forms.

Theorem 1. *Suppose that $f(b)$ does not vanish. Then for the largest prime divisor p_n in the nominator of S_n holds*

$$\limsup_{n\to\infty} p_n = \infty.$$

The condition $f(b) \neq 0$ in this theorem is necessary, as is shown by the example

$$f(z) = 1 - \sum_{1}^{\infty} 2^{-n} z^n,\ b = 1,\ S_n = 2^{-n}.$$

We obtain a much sharper result if we add a further condition:

Theorem 2. *Suppose that $f(b)$ is an irrational number, then $p_n \to \infty$ if $n \to \infty$.*

If $f(z)$ represents a rational function then one easily shows that $f(b)$ is always a rational number (compare footnote [1]) in section 2) and thus it is not possible to apply theorem 2 in this case. However, if $f(z)$ represents an algebraic function of degree $\geqslant 2$, then by a well-known theorem of HILBERT [2], p. 129, any interval in $-R < x < R$, however small, contains a rational number b such that $f(b)$ is irrational and by a result of DÖRGE [1], p. 93–94, $f(b)$ is irrational for "almost every" rational number b in $-R < x < R$, if "almost every" is taken in a certain sense.

For rational functions, as is said before, it is not possible to apply theorem 2. However, in this case we have the following result:

Theorem 3. *Let $f(z)$ be the Taylor series of a rational function. Let its poles $\omega_1, \omega_2, \ldots, \omega_r$ have the property that none of the quotients $\omega_i : \omega_j$ $(1 \leqslant i < j \leqslant r)$ is a root of unity. Suppose that $f(b) \neq 0$. Then $p_n \to \infty$ if $n \to \infty$.*

We remark that these theorems "generalize themselves"; indeed $f'(z) = \sum_1^\infty n a_n z^{n-1}$ again represents an algebraic function, is not a polynomial, has rational coefficients and converges for $|z| < R$. Hence we can apply the theorems 1–3 to $f'(z)$ instead of to $f(z)$. Thus from theorem 2 e.g. it follows: "Suppose that $f'(b)$ is an irrational number, then for the largest prime divisor p_n^* of the nominator in $\sum_{\nu=1}^{n} \nu a_\nu b^{\nu-1}$ holds $p_n^* \to \infty$ if $n \to \infty$".

It is very important that we can apply the theorems 1–3 to the problem stated above. This we will do in section 3. However, we can solve this problem only in rather special cases. The power series $\sum_1^\infty a_n z^n$ we consider,

have rational coefficients, represent a branch of an algebraic function with a single singularity on its circle of convergence. This singularity is a pole $z=b$ of the first order and b is a rational number. We get results corresponding to the theorems 1–3. For instance corresponding to theorem 2 we obtain: If the residual of the pole $z=b$ is an irrational number, then the largest prime divisor in the nominator of a_n must tend to infinity if n increases indefinitely.

As an application of one of the results obtained in section 3 we give here a very simple example: Let a, b, c, d be non-vanishing integers, $|b|>|d|$. Then the largest prime divisor of ab^n+cd^n tends to infinity if n increases indefinitely.

2. Proofs of the theorems 1–3.

The Thue–Siegel–Roth theorem states:

Let α denote a real algebraic number and let k be any real number >2. Then the inequality

$$0<\left|\alpha-\frac{x}{y}\right|<y^{-k}$$

has at most a finite number of solutions in integers x and $y>0$.

Recently Ridout [8] has given a generalization of this theorem: By imposing further conditions on the integers x and y it is possible to reduce the lower bound 2 for k. For our purpose we need only the following very special case of Ridout's result:

Let $\alpha\neq 0$ denote a real algebraic number, let k be any positive number and let $P_1, P_2, \ldots, P_w$ be given primes. We restrict the integers x and $y>0$ to numbers with at most $P_1, P_2, \ldots, P_w$ as prime divisors:

$$x=\pm P_1^{\xi_1}P_2^{\xi_2},\ldots,P_w^{\xi_w},\ y=P_1^{\eta_1}P_2^{\eta_2}\ldots P_w^{\eta_w}, \tag{1}$$

where the ξ's and η's are non-negative integers.

Then the inequality

$$0<\left|\alpha-\frac{x}{y}\right|<y^{-k} \tag{2}$$

has at most a finite number of solutions in these x and y.

For Ridout's complete theorem and the deduction of this special case from it see the appendix.

Proof of theorem 2. We divide the proof into four parts.

a) Put $b=u/v$, where u and $v>0$ are integers, then $S_n=\sum_{\nu=0}^{n}a_\nu(u^\nu/v^\nu)$. From Eisenstein's theorem we derive the existence of a positive integer N such that the $N^n a_n$ $(n=1, 2, \ldots)$ are integers. Let N_0 be the denominator of a_0. Then S_n can be written

$$S_n=\frac{x_n}{y_n}\ \text{with}\ y_n=(N_0Nv)^n \tag{3}$$

and x_n an integer for $n\geqslant 1$. Denote the prime divisors of N_0Nv by $P_1, P_2, \ldots, P_g$.

Let us now suppose that the assertion $p_n \to \infty$ is false. Then there exists a monotonically increasing sequence of positive integers $\{n_i\}_{i=1}^{\infty}$ such that all the nominators of S_{n_i} can be formed from a finite number of primes $P_{g+1}, P_{g+2}, \ldots, P_w$. It follows from (3) that $P_1, P_2, \ldots, P_w$ *are the only possible prime divisors in* y_{n_i} *as well as in* x_{n_i}:

$$x_{n_i} = \pm P_1^{\xi_1} \ldots P_w^{\xi_w}, \; y_{n_i} = P_1^{\eta_1} \ldots P_w^{\eta_w}$$

where the ξ's and η's are non-negative integers.

b) $f(z)$ satisfies an algebraic equation

$$\sum_{\mu=0}^{m} P_\mu(z) f^\mu(z) = 0, \tag{4}$$

where the $P_\mu(z)$ are polynomials. Now all coefficients a_n in $f(z)$ are rationals, therefore by a well-known argument (see e.g. PÓLYA and SZEGÖ [6], Aufgabe 150, p. 141) we may assume without loss of generality that the polynomials $P_\mu(z)$ have rational coefficients [1]). Also we may assume that $P_\mu(b) \neq 0$ for at least one value of $\mu = 1, 2, \ldots, m$. Putting $z = b$ in (4) we derive that

$$\alpha \overset{\text{def}}{=} f(b) \; \textit{is algebraic} \neq 0.$$

c) We have $|b| < R$, hence there exists a positive number δ so small that

$$\omega \overset{\text{def}}{=} (R^{-1} + \delta)|b| < 1.$$

If $R' (\geqslant R)$ denotes the radius of convergence of $\sum a_n z^n$, then

$$\limsup \sqrt[n]{|a_n|} = (R')^{-1}.$$

Hence for sufficiently large n_i we have on account of (3)

$$\left| \alpha - \frac{x_{n_i}}{y_{n_i}} \right| = \left| \sum_{n_i+1}^{\infty} a_\nu b^\nu \right| \leqslant \sum_{n_i+1}^{\infty} (R^{-1} + \delta)^\nu |b|^\nu = \frac{\omega^{n_i+1}}{1-\omega}.$$

Choose a positive number k so small that

$$(N_0 N v)^{-k} > \omega,$$

then for sufficiently large n_i

$$y_{n_i}^{-k} = (N_0 N v)^{-k n_i} > \frac{\omega^{n_i}}{1-\omega},$$

hence for sufficiently large n_i

$$\left| \alpha - \frac{x_{n_i}}{y_{n_i}} \right| < \frac{\omega^{n_i}}{1-\omega} < y_{n_i}^{-k}.$$

---

[1]) From this it follows that, if $f(z)$ represents a rational function, $f(b)$ must necessarily be a rational number.

d) Now, using the results obtained in a), b) and c) we are in a position to apply Ridout's result as stated in the beginning of this proof. It follows

$$\alpha = \frac{x_{n_i}}{y_{n_i}} \text{ for sufficiently large } n_i.$$

However, this means that $\alpha = f(b)$ is rational; this contradicts the condition that $f(b)$ must be irrational and thus the assertion $p_n \to \infty$ must be true.

Proof of theorem 1. The method we used in the proof of theorem 2 is also applicable in this case if we take $\{n_i\}_{i=1}^{\infty} = \{i\}_{i=1}^{\infty}$. For let us suppose that the assertion lim sup $p_n = \infty$ of theorem 1 is false. Then all numbers y_i, x_i have a finite number of prime divisors $P_1, P_2, \ldots, P_w$ and we find by a similar reasoning as before

$$\alpha = f(b) = \frac{x_i}{y_i} \text{ for sufficiently large } i.$$

It follows

$$a_i b^i = S_i - S_{i-1} = 0, \text{ hence } a_i = 0, \text{ for sufficiently large } i,$$

so that $f(z)$ is necessarily a polynomial, and this provides a contradiction.

Proof of theorem 3. We now need the following well-known theorem about rational functions.

Let in a Taylor series $\sum_1^{\infty} a_n z^n$ of a rational function infinitely many coefficients vanish; let all vanishing coefficients be represented by

$$a_{n_1} = a_{n_2} = \ldots = 0,$$

where the sequence $\{n_i\}_{i=1}^{\infty}$ increases monotonically. Then from some index i_0 on this sequence is periodical; i.e. there exists a positive integer L such that if n_i $(i \geqslant i_0)$ belongs to the sequence then the same assertion holds for $n_i + L$.

Special cases of this beautiful theorem were proved by SIEGEL [10], WARD [12], SKOLEM [11] and MAHLER [4]. The most general result is due to MAHLER [5] and LECH [3].

From this theorem it follows easily (see MAHLER [5], p. 40):

Let for a rational function, not a polynomial, the poles $\omega_1, \omega_2, \ldots, \omega_r$ have the property that none of the quotients $\omega_i : \omega_j$ $(1 \leqslant i < j \leqslant r)$ is a root of unity, then at most a finite number of Taylor coefficients can vanish.

For the proof of theorem 3 we use the same method as in the proof of theorem 2. Suppose that the assertion $p_n \to \infty$ is false. We find as before a monotonically increasing sequence $\{n_i\}_{i=1}^{\infty}$ such that for sufficiently large i, say for $i \geqslant g$,

$$S_{n_i} = \sum_{\nu=0}^{n_i} a_\nu b^\nu = \alpha = f(b),$$

hence

$$\sum_{n_g+1}^{n_i} a_\nu b^\nu = 0 \qquad (i = g+1, g+2, \ldots). \tag{5}$$

Now $\sum_0^n a_\nu b^\nu$ is the Taylor coefficient of z^n in the expansion of

$$\frac{f(bz)}{1-z} = \sum_{\nu=0}^{\infty} z^\nu \cdot \sum_{\nu=0}^{\infty} a_\nu b^\nu z^\nu.$$

Similarly (5) is the coefficient of z^{n_i} in the expansion of the rational function

$$F(z) = \frac{\sum_{n_g+1}^{\infty} a_\nu b^\nu z^\nu}{1-z} = \frac{f(bz) - \sum_0^{n_g} a_\nu b^\nu z^\nu}{1-z}.$$

This rational function has an infinity of vanishing Taylorcoefficients. On the other hand its poles $b^{-1}\omega_1, b^{-1}\omega_2, \ldots, b^{-1}\omega_r$ have the property that none of the quotients is a root of unity. We get thus a contradiction, hence the assertion $p_n \to \infty$ is true.

By the same method one is led to the following somewhat more general result.

Theorem 4. *Let the joint conditions of the theorems* 1–3 *stated in section* 1 *be satisfied and let moreover* $f(z)$ *be the Taylor series of a rational function* $f(z)$ *with the property* $f(b) \neq 0$. *Suppose that a monotonically increasing sequence* $\{n_i\}_{i=1}^{\infty}$ *of positive integers exists, such that the nominators of the* S_{n_i} *have at most a finite number of prime divisors, then the sequence* $\{n_i\}_{i=1}^{\infty}$ *must be periodic from some index* i_0 *on.*

3. In this section we apply the theorems 1–4 to our problem about the nominators of the Taylorcoefficients of algebraic functions.

First we enunciate the joint conditions of our theorems:

Let the power series

$$f(z) = \sum_0^{\infty} a_n z^n \tag{6}$$

with rational coefficients a_n *represent a branch of an algebraic function. Let this branch have a pole of the first order as its only singularity on the circle of convergence of* (6). *Let this pole* $z = b$ *represent a rational number. We shall always exclude the case that* $f(z)$ *has the form*

$$\frac{\text{polynomial in } z}{z-b}.$$

By "translating" the theorems 1–4 we get the following corresponding results:

Theorem I. *If* p_n *denotes the largest prime divisor in the nominator of* a_n, *then*

$$\limsup_{n \to \infty} p_n = \infty.$$

Theorem II. *Let the residual for the pole* $z = b$ *be an irrational number. then* $p_n \to \infty$ *if* $n \to \infty$.

Theorem III. *Let* (6) *represent the Taylor series of a rational function with poles* $\omega_1, \omega_2, \ldots, \omega_r$. *Let the quotient of two different poles never be a root of unity. Then* $p_n \to \infty$ *if* $n \to \infty$.

Theorem IV. *Let* (6) *represent the Taylor series of a rational function. Suppose that a monotonically increasing sequence* $\{n_i\}_{i=1}^{\infty}$ *of positive integers exists, such that the nominators of the* a_{n_i} *have at most a finite number of prime divisors, then the sequence* $\{n_i\}_{i=1}^{\infty}$ *must be periodic from some index* i_0 *on.*

The proofs of these theorems are similar. As an example we give the proof of theorem II:

The function

$$F(z) \overset{\text{def}}{=} (1 - b^{-1}z) f(z)$$

is regular for $|z| \leqslant |b|$ and can be written

$$F(z) = \sum_0^{\infty} \alpha_n z^n$$

with rational coefficients α_n.

If ϱ denotes the irrational residual of $f(z)$ for the pole $z = b$, then one finds easily

$$F(b) = -b^{-1}\varrho = \textit{irrational.}$$

Now we can apply theorem 2 with $F(z)$ instead of $f(z)$. It follows that the largest prime divisor in the nominator of $\sum_0^n \alpha_\nu b^\nu$ tends to infinity if $n \to \infty$.

On the other hand $\sum_0^n \alpha_\nu b^\nu$ is the coefficient of z^n in the Taylor expansion of $\frac{F(bz)}{1-z} = f(bz)$, hence

$$\sum_0^n \alpha_\nu b^\nu = a_n b^n$$

and the assertion of our theorem II follows.

For sufficiently large n the Taylorcoefficients a_n of a rational function $f(z)$ have a representation

$$a_n = \sum_{\varrho=1}^{r} P_\varrho(n) \lambda_\varrho^n, \tag{7}$$

where $\lambda_1^{-1}, \lambda_2^{-1}, \ldots, \lambda_r^{-1}$ represent the poles of $f(z)$ and where the $P_\varrho(z)$ are polynomials in z of degree $m_\varrho - 1$, m_ϱ denoting the order of the pole λ_ϱ^{-1}.

Conversely, if a_n is given by (7) for $n = 0, 1, 2, \ldots$, then

$$f(z) = \sum_0^{\infty} a_n z^n$$

represents a rational function with the poles $\lambda_1^{-1}, \lambda_2^{-1}, \ldots, \lambda_r^{-1}$, respectively of orders $m_1, m_2, \ldots, m_r$.

Now consider a function

$$g(x) = A\lambda_1^x + \sum_{\varrho=2}^{r} P_\varrho(x)\,\lambda_\varrho^x$$

where the constant $A \neq 0$ *and where the polynomials* $P_\varrho(x)$ *do not vanish identically, such that all numbers* $g(n)$ *are rationals* $(n = 0, 1, 2, \ldots)$. *Let* $r \geqslant 2$, λ_1 *be a rational number such that*

$$|\lambda_1| > |\lambda_\varrho| > 0 \text{ for } \varrho = 2, 3, \ldots, r.$$

Then we obtain from theorem III:

Theorem V. *Let moreover none of the quotients* $\lambda_i : \lambda_j$ $(2 \leqslant i < j \leqslant r)$ *be a root of unity. If* p_n *denotes the largest prime divisor in the nominator of* $g(n)$, *then* $p_n \to \infty$ *if* $n \to \infty$.

From theorem IV we deduce:

Theorem VI. *Suppose that a monotonically increasing sequence* $\{n_i\}_{i=1}^{\infty}$ *exists, such that the nominators of* $g(n_i)$ *have at most a finite number of prime divisors, then the sequence* $\{n_i\}_{i=1}^{\infty}$ *must be periodic from some index* i_0 *on.*

As an example for theorem V we find:

Let a, b, c, d *be integers* $\neq 0$, *let* $|b| > |d|$, *then the largest prime divisor of* $ab^n + cd^n$ *tends to infinity if* n *increases indefinitely.*

4. Appendix. Ridout's theorem:

Let α be any algebraic number other than 0; let $P_1, P_2, \ldots, P_s$, $Q_1, Q_2, \ldots, Q_t$ be distinct primes; and let μ, ν, c be real numbers satisfying

$$0 \leqslant \mu \leqslant 1, \quad 0 \leqslant \nu \leqslant 1, \quad c > 0.$$

Let x, y be restricted to integers of the form

$$x = x^* P_1^{\varrho_1} \ldots P_s^{\varrho_s}, \; y = y^* Q_1^{\sigma_1} \ldots Q_t^{\sigma_t}$$

where $\varrho_1, \ldots, \varrho_s, \; \sigma_1, \ldots, \sigma_t$ are non-negative integers and x^*, y^* are integers satisfying

$$0 < |x^*| \leqslant c|x|^\mu, \quad 0 < y^* \leqslant cy^\nu.$$

Then if

$$k > \mu + \nu,$$

the inequality

$$0 < \left| \alpha - \frac{x}{y} \right| < y^{-k}$$

has at most a finite number of solutions in x, y.

It is easy to deduce from this theorem the result used in section 2. Suppose that, contrary to the assertion there, the inequality (2) has an infinite number of different solutions x, y of the form (1). Then it is clear that we also have infinitely many different solutions x, y of (2) of the form (1) such that $(x, y) = 1$. We confine ourselves to these solutions. If

P_i is a divisor of x, then P_i is not a divisor of y. Thus every solution x, y with $(x, y) = 1$ splits the set of primes $P_1, \ldots, P_w$ into two subsets. In the first subset we put all numbers P_i $(i = 1, \ldots, w)$ which are divisors of x, in the second the remaining numbers. There is at least one division into subsets which occurs infinitely often. The distinct primes in the first subset are, say, $P_1, \ldots, P_s$, those in the second $Q_1, Q_2, \ldots, Q_t$. Hence we have infinitely many solutions x, y of the inequality (2) of the form

$$x = \pm P_1^{\varrho_1} \ldots P_s^{\varrho_s}, \; y = Q_1^{\sigma_1} \ldots Q_t^{\sigma_t},$$

where the ϱ's and σ's are non-negative integers. However, application of Ridout's theorem with $\mu = \nu = 0$, $c = 1$, $x^* = \pm 1$, $y^* = 1$ shows that there is at most a finite number of solutions of the inequality (2) of this form. This gives a contradiction and the assertion must be true.

REFERENCES

1. Dörge, K., Zum Hilbertschen Irreduzibilitätssatz, Math. Annalen, **95**, 84–97 (1926).
2. Hilbert, D., Ueber die Irreducibilität ganzer rationalen Functionen mit ganzzahligen Coefficienten, J. f. reine u. angew. Math., **110**, 104–129 (1892).
3. Lech, C., A note on recurring series, Arkiv för Matematik, **2**, 417–421 (1954).
4. Mahler, K., Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen, Proc. Akad. Wetensch., Amsterdam, **38**, 51–60 (1935).
5. ————, On the Taylorcoefficients of rational functions, Proc. Cambridge Phil. Soc., **52**, Part 1, 39–48 (1956).
6. Pólya, G. und G. Szegö, Aufgaben und Lehrsätze aus der Analysis, II, New York 1945.
7. Pólya, G., Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, J. f. reine u. angew. Math., **151**, 1–31 (1921).
8. Ridout, D., Rational approximations to algebraic numbers, Mathematika **4**, 125–131 (1957).
9. Siegel, C. L., Approximation algebraischer Zahlen, Math. Z., **9**, 173–213 (1921) (p. 207, Satz 8)
10. ————, Ueber die Coefficienten in der Taylorschen Entwicklung rationaler Functionen, Tôhoku Math. J., **20**, 26–31 (1921).
11. Skolem, Th., Einige Sätze über gewisse Reihenentwicklungen usw., Skr. Norske Vidensk. Akad., **6** (1933).
12. Ward, M., Note on a arithmetical property of recurring series, Math. Z. **39**, 211–214 (1935).