Finally we remark that there is no difference between the case $k = 1$ and the general one but for the fact that there is no need to subdivide the zeros with $|\gamma| > 1/\theta$ in (10).

References

[1] E. Bombieri and H. Davenport, *Small differences between prime numbers*, Proc. Roy. Soc. Ser. A 293 (1966), pp. 1–18.
[2] H. Cramér, *Some theorems concerning prime numbers*, Ark. Mat. Astronom. Fys. 15 (5) (1920).
[3] P. X. Gallagher, *On the distribution of primes in short intervals*, Mathematika 23 (1976), pp. 4–9.
[4] D. R. Heath-Brown and H. Iwaniec, *On the difference between consecutive primes*, Invent. Math. 55 (1979), pp. 49–69.
[5] M. N. Huxley, *On the difference between consecutive primes*, ibid. 15 (1972), pp. 164–170.
[6] A. E. Ingham, *On the difference between consecutive primes*, Quart. Journ. Math. 8 (1937), pp. 255–266.
[7] H. Iwaniec and M. Jutila, *Primes in short intervals*, Ark. Mat. 17 (1979), pp. 167–176.
[8] A. F. Lavrik, *On the theory of distribution of primes, based on I. M. Vinogradov's method of trigonometrical sums* (Russian), Trudy Mat. Inst. Steklov 64 (1961), pp. 90–125.
[9] B. Saffari and R. C. Vaughan, *On the fractional parts of x/n and related sequences*, Ann. Inst. Fourier 27 (1977), pp. 2–30.
[10] A. Selberg, *On the normal density of primes in small intervals, and the difference between consecutive primes*, Arch. Mat. Naturvid. 47 (1943), pp. 87–105.

SCUOLA NORMALE SUPERIORE
56100 Pisa, Italy
ISTITUTO DI INGEGNERIA
FACOLTÀ DI SCIENZE M. F. N.
84081 Baronissi (SA), Italy

Received on 24.2.1981 (1242)

ACTA ARITHMETICA
XLII (1982)

On a conjecture of D. H. Lehmer

by

D. C. Cantor and E. G. Straus* (Los Angeles, Calif.)

1. Introduction. K. Mahler assigned the measure

$$M(\theta) = \prod_{i=1}^{d} \max\{1, |\theta_i|\}$$

to the algebraic integer θ of degree d with conjugates $\theta_1, \ldots, \theta_d$. D. H. Lehmer conjectured that there is a constant $c > 1$ so that $M(\theta) < c$ implies that θ is a root of unity. While Lehmer's conjecture remains unproved, there has been significant progress in giving lower bounds depending on the degree d for $M(\theta)$. Recently E. Dobrowolski [1] has shown that there exists a positive constant $c > 0$ such that $M(\theta) < 1 + c(\log\log d/\log d)^3$ implies that θ is a root of unity.

In this note we follow Dobrowolski's ideas and obtain a somewhat simpler proof of his result coupled with an improvement on the constant.

THEOREM. *If $c < 2$ then for all sufficiently large d the inequality*

$$M(\theta) < 1 + c(\log\log d/\log d)^3$$

implies that the algebraic integer θ of degree d is a root of unity.

Our main tool is an estimation of a Vandermonde determinant which is constructed so as to have a large integral divisor. If $M(\theta)$ is too small, this Vandermonde vanishes, proving that θ is a root of an algebraic integer of lower degree.

2. Proof of theorem. Suppose n is a positive integer and a is a complex number. Define the (column) vectors

$$v_0(a) = (1, a, a^2, \ldots, a^{n-1})^t$$

* This material is based upon work supported by the National Science Foundation under Grants MCS79-0311 and MCS79-03162.

and

$$v_i(\alpha) = \frac{1}{i!}\frac{d^i}{d\alpha^i}v_0(\alpha) = \left(\binom{0}{i}\alpha^{-i}, \binom{1}{i}\alpha^{1-i}, \ldots, \binom{n-1}{i}\alpha^{n-1-i}\right)^t,$$

(as usual we set $\binom{h}{i} = 0$ if h is an integer $< i$).

Now suppose $\boldsymbol{a} = (a_1, a_2, \ldots, a_m)$ is an m-dimensional vector of complex numbers and $\boldsymbol{r} = (r_1, r_2, \ldots, r_m)$ is an m-dimensional vector of positive integers. Put $n = \sum_{i=1}^m r_i$ and define the (confluent) Vandermonde determinant $V(\boldsymbol{a}; \boldsymbol{r})$ to be the n by n determinant whose columns are the vectors $v_i(a_j)$, where $1 \leqslant j \leqslant m$ and $0 \leqslant i \leqslant r_j - 1$; the ordering of columns is irrelevant. The following is well-known [2].

LEMMA 1. *The determinant* $V(\boldsymbol{a}; \boldsymbol{r}) = \mp \prod_{i<j}(a_i - a_j)^{r_i r_j}$, *where the product is over all ordered pairs* (i, j) *satisfying* $1 \leqslant i < j \leqslant m$. ∎

Next note that

$$\|v_i(a_j)\|_2^2 = \sum_{k=i}^{n-1}\binom{k}{i}^2 |a_j|^{2(k-i)}$$
$$\leqslant \max(1, |a_j|)^{2n}\sum_{k=i}^{n-1}\binom{k}{i}^2 \leqslant n^{2i+1}\max(1, |a_j|^{2n}).$$

Thus from Hadamard's inequality we obtain the following.

LEMMA 2. *We have*

$$|V(\boldsymbol{a}, \boldsymbol{r})|^2 \leqslant \prod_{j=1}^m \max(1, |a_j|)^{2r_j n} n^{r_j^2}. \ \blacksquare$$

We now prove the theorem. Suppose that θ is an algebraic integer of degree d and that $\theta_1, \ldots, \theta_d$ are its conjugates, considered as complex numbers, with

$$M = M(\theta) = \prod_{i=1}^d \max(1, |\theta_i|).$$

Put $p_0 = 1$ and let $p_1, p_2, \ldots, p_s$ denote the first s primes.

Now let k be a positive integer and define

$$\boldsymbol{a} = (\theta_1^{p_0}, \theta_2^{p_0}, \ldots, \theta_d^{p_0}, \theta_1^{p_1}, \theta_2^{p_1}, \ldots, \theta_d^{p_1}, \ldots, \theta_1^{p_s}, \theta_2^{p_s}, \ldots, \theta_d^{p_s})$$

and

$$\boldsymbol{r} = (k, k, \ldots, k, 1, 1, \ldots, 1)$$

(here the first d elements are k, and the remaining sd elements are 1). With this choice of $\boldsymbol{a}$ and $\boldsymbol{r}$, and $n = (k+s)d$, Lemma 2 yields

$$|V|^2 \leqslant n^{d(k^2+s)} M^{2(k+p_1+p_2+\ldots+p_s)n}$$

where $V = V(\boldsymbol{a}, \boldsymbol{r})$. In terms of logarithms the inequality becomes

$$2n(k+p_1+p_2+\ldots+p_s)\log M + d(k^2+s)\log n \geqslant 2\log|V|. \tag{1}$$

Put $f(z) = \prod_{i=1}^d (z - \theta_i)$ and note that if p is prime, then $f(z^p) \equiv f(z)^p \pmod p$ and hence $f(\theta_i^p) \equiv f(\theta_i)^p \equiv 0 \pmod p$.

Thus p^d divides the integer

$$\prod_{i=1}^d f(\theta_i^p) = \prod_{i=1}^d\prod_{j=1}^d (\theta_i^p - \theta_j).$$

Now V^2 is an integer divisible by

$$\prod_{i=1}^d\prod_{j=1}^d (\theta_i^{p_h} - \theta_j)^{2k}, \quad 1 \leqslant h \leqslant s;$$

hence V^2 is divisible by $\prod_{j=1}^s p_j^{2dk}$ and either $V = 0$ or

$$2\log|V| \geqslant 2dk\sum_{j=1}^s \log p_j. \tag{2}$$

Combining (1) and (2) yields: If $V \neq 0$ then

$$\log M \geqslant \frac{2dk\sum_{j=1}^s \log p_j - d(k^2+s)\log n}{2n\left(k + \sum_{j=1}^s p_j\right)} = \frac{2k\sum_{j=1}^s \log p_j - (k^2+s)\log n}{2(k+s)\left(k + \sum_{j=1}^s p_j\right)}. \tag{3}$$

We may assume $d \geqslant 4$ and put $r = \log d$, then choose $k = [r/\log r]$ and $s = [(r/\log r)^2/2]$. The prime number theorem yields

$$\sum_{j=1}^s \log p_j = s\log s(1+o(1)),$$
$$\sum_{j=1}^s p_j = \tfrac{1}{2}s^2\log s(1+o(1)).$$

Substitution in (3) yields

$$\log M \geqslant \frac{\big(2ks\log s - (k^2+s)\log(d(k+s))\big)(1+o(1))}{2(k+s)(k+s^2\log s/2)} \tag{4}$$
$$= \frac{\big(2r^3/(\log r)^2 - (3/2)r^3/(\log r)^2\big)(1+o(1))}{2\cdot\frac{1}{2}\left(\frac{r}{\log r}\right)^2\left(\frac{1}{4}\frac{r^4}{(\log r)^3}\right)}$$
$$= 2\left(\frac{\log r}{r}\right)^3(1+o(1)) = 2\left(\frac{\log\log d}{\log d}\right)^3(1+o(1)).$$

Suppose $c < 2$ and

$$\log M < c(\log\log d/\log d)^3.$$

Then for sufficiently large d, inequality (4) implies $V = 0$ and hence $\theta_h^{p_i} = \theta_j^{p_k}$ for some h, i, j, k. If $i \neq k$, say $i < k$, then there is an automorphism σ of $Q(\theta_1, \theta_2, \ldots, \theta_d)$ such that $\sigma\theta_j = \theta_h = \theta_j^{p_k/p_i}$. If $|\theta_j| \neq 1$ then $\sigma^m\theta_j$ approaches 0 or ∞ as $m \to \infty$. This is impossible and hence $|\theta_j| = 1$. Conjugation of the equation $\theta_h^{p_i} = \theta_j^{p_k}$ shows that all of the θ_i have absolute value 1, hence they are roots of unity, by Kronecker's theorem. If $p_i = p_k = p$, then θ_h/θ_j is a pth root of unity, and $M(\theta) = M(\theta^p)$ where θ^p is an algebraic integer of degree d/p. For each $d > 1$ there exist only finitely many algebraic integers Θ of degree d satisfying $M(\Theta) < 2$. Thus there exists a function $H(\Theta) > 1$, such that if $M(\Theta) < H(\Theta)$ then Θ is a root of unity, and then $V(\boldsymbol{a}, \boldsymbol{r}) = 0$. Hence there exists a monotonically decreasing function $G(\Theta)$ such that if $\log M(\Theta) < G(\Theta)$, then $V(\boldsymbol{a}, \boldsymbol{r}) = 0$. By what we have shown, we can choose $G(\Theta) = c(\log\log d/\log d)^3$ for all sufficiently large d. Now if Θ has degree d and $\log M(\Theta) < G(\Theta)$, then either Θ is a root of unity or there exists a prime p such that Θ^p has degree d/p and $\log M(\Theta^p) = \log M(\Theta) < G(d) < G(d/p)$.

This completes the proof by induction. We have tried improved estimates of the Vandermonde and variations in the choices of its column vectors. While we can improve the error term in

$$M(\Theta) > 1 + 2(\log\log d/\log d)^3 + o\big((\log\log d/\log d)^3\big),$$

if Θ is not a root of unity, none of the changes improves the constant 2.

References

[1] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), pp. 391–401.

[2] Ch. Méray, *Sur un déterminant dont celui de Vandermonde n'est qu' un cas particulier*, Revue de Mathématiques Spéciales, 9 (1899), pp. 217–219.

UNIVERSITY OF CALIFORNIA
Los Angeles, CA 90024
USA

Received on 10.4.1981
and in revised form on 5.5.1981 (1249)

ACTA ARITHMETICA
XLII (1982)

Courbes définies sur les corps de séries formelles et loi de réciprocité

par

J. C. Douai et C. Touibi (Tunis)

Introduction. Soit k_0 un corps algébriquement clos de caractéristique quelconque, Rim et Whaples ([5]) ont montré que pour les corps de fonctions définies sur $k = k_0((T))$ il n'y a pas en général de loi de réciprocité. (On dit que la loi de réciprocité est valable sur le corps k si pour tout corps de fonctions d'une variable K sur k, l'application norme résiduelle induit l'isomorphisme:

$$(*, L|K): C_K|NC_L \to \mathrm{Gal}(L|K)$$

pour toutes les extensions abéliennes finies L de K, où C_K désigne le groupe des classes d'idéles et où $N = N_{L|K}$ est la norme.)

En fait, les corps qu'ils considèrent sont des corps de fonctions de courbes dont le genre est strictement positif et qui ont „relativement bonne réduction" mod T, i.e. dont la courbe réduite est encore de genre strictement positif ([5], corollaire du théorème 2).

Le but de ce travail est de montrer que si X est une courbe régulière, complète, irréductible, définie sur k et dont la jacobienne a „très mauvaise réduction" mod T, i.e. la réduite mod T est de type additif, alors la loi de réciprocité est valable pour le corps de fonction $k(X)$.

Plus précisément, en combinant un résultat de Ogg [4] avec un résultat de Rim et Whaples [5], on obtient:

THÉORÈME. *Soit X une courbe algébrique, irréductible, lisse, complète, définie sur un corps de séries formelles $k = k_0((T))$ où k_0 est un corps algébriquement clos de caractéristique nulle. Si la jacobienne de X a „très mauvaise réduction" mod T alors la loi de réciprocité est valable pour le corps de fonctions $k(X)$.*

Nous montrons même que dans la situation considérée, ceci est le seul cas où la loi de réciprocité est valable.