ว.เกษตรศาสตร์ (วิทย.) 25 : 484 - 488 (2534)

Approximation of Exponentials in the p-Adic Domain

Vichian Laohakosol[1]

ABSTRACT

Using a method first developed by Hermite and later improved by Mahler, we establish lower bounds for the approximation of p-adic exponential functions evaluated at rational points.

INTRODUCTION

In 1873, Hermite (1873) gave a proof of transcendence of the exponential value e. Since then his method has been extensively refined and further developed, notably by Siegel and Mahler. Specifically, Mahler (1932) successfully employed this method to prove the algebraic independence of exponential functions evaluated at algebraic points (first proved by Lindemann) as well as giving the measure of algebraic independence. More precise lower bounds on the approximation of an exponential function evaluated at rational points have also been obtained via this method; see e.g. Durand (1980). On the other hand, results related to algebraic independence of p-adic exponential functions have previously been obtained in Serre (1965/66), Waldschmidt (1973) and Bundschuh and Wallisser (1979).

Stimulated by the works of Mahler (1932, 1967), in the present paper, we use an analogous method developed in the p-adic fields to prove the following result.

Theorem Let $0 = \omega_0 < \omega_1 < \ldots < \omega_m = \Omega$ be distinct rational integers; ρ, v and b be positive integers; a be rational integral with g.c.d. (a,p) = g.c.d. (b,p) = 1; q_0 (≥ 1), $q_1, \ldots, q_m$ be m+1 arbitrary rational integers with $q = \max(|q_0|, |q_1|, \ldots, |q_m|)$. If

$$\rho\, p^{1-(m+1)\rho v + mp/(p-1)} \leq 1/S\, |q_0|_p ,$$

then

$$\max_{k=1,\ldots,m} \left| q_0 e^{\omega_k p^v a/b} - q_k \right|_p > 1/S ,$$

where $S = S(p,\rho,\Omega,q,m,v,a,b) = 2(m+1)\, b^{\rho}\, (13 \rho m^{\Omega} e^{6\Omega})^{\rho} (\rho+1)\, q\, (1 + |p^v a/b|^{\rho})$.

MATERIALS AND METHODS

Notation Throughout the whole paper

p denotes a fixed rational prime.

IN denotes the set of natural numbers.

ZZ denotes the ring of rational integers.

$| \; |$ denotes the usual absolute valuation.

$| \; |_p$ denotes the p-adic valuation so normalized that $|p|_p = 1/p$.

$\mathbb{C}_p$ denotes the completion of the algebraic closure of $\mathbb{Q}_p$, the p-adic field.

m, $\rho_0, \rho_1, \ldots, \rho_m$ are positive integers with $\sigma = \rho_0 + \rho_1 + \ldots + \rho_m - 1$.

Let $\omega_0, \omega_1, \ldots, \omega_m$ be distinct elements of $\mathbb{C}_p$ satisfying

$$|\omega_k|_p \leq 1 \qquad (k = 0, 1, \ldots, m).$$

Let z in $\mathbb{C}_p$ be such that $|z|_p = p^{-1/(p-1) - \theta}$ where $\theta = \theta(z)$ is a positive real number.

From linear algebra, we have the following facts (see e.g. LeVeque (1956) or Mahler (1932)).

(i) There exist m+1 polynomials $A_k(z,\omega,\rho) = A_k(z, \omega_0, \ldots, \omega_m, \rho_0, \ldots, \rho_m)$ ($k = 0, 1 \ldots, m$) not all

1 Dept. of Mathematics, Faculty of Science, Kasetsart University, Bangkok 10900, Thailand.

identically zero of degrees at most ρ_0-1, ρ_1-1, . . ., ρ_m -1, respectively, such that the analytic function

$$R(z,\omega,\rho) = R(z,\omega_0,\ldots,\omega_m,\rho_0,\ldots,\rho_m) := \sum_{k=0}^{m} A_k(z,\omega,\rho)e^{\omega_k z}$$

vanishes at $z = 0$ up to order σ.

(ii) If

$R(z,\omega,\rho) := Cz^{\sigma}$ + higher powers of z, is the analytic function mentioned in (i), then $C \neq 0$.

Assumption From now on, we always take the value C in (ii) above to be $C = 1/\sigma!$, and so $R(z,\omega,\rho)$ and $A_k(z,\omega,\rho)$ are always uniquely determined.

As seen from Bundschuh and Wallisser (1979), Mahler (1932, 1967), most analytic identities involving $A_k(z,\omega,\rho)$ and $R(z,\omega,\rho)$ are actually universal algebraic identities, valid over any field of zero characteristic, in particular T_ρ, and indeed explicit formulae for $A_k(z,\omega,\rho)$ and $R(z,\omega,\rho)$ are given by (see p. 186 of Bundschuh and Wallisser (1979), pp. 124-125 of Mahler (1932) or p. 203 of Mahler (1967))

$$A_k(z,\omega,\rho) = \left(\prod_{\substack{i=0\\ i\neq k}}^{m}(\omega_k-\omega_i)^{-\rho_k}\right)\left(\prod_{\substack{i=0\\ i\neq k}}^{m}\left(\sum_{\lambda=0}^{\infty}\binom{-\rho_k}{\lambda}(\omega_k-\omega_i)^{-\lambda}D_z^{\lambda}\right)\frac{z^{\rho_k-1}}{(\rho_k-1)!}\right) \quad .....(1)$$

where $D_z = d/d_z$, and

$$R(z,\omega,\rho) = \sum_{n=0}^{\infty} a_n z^{n+\sigma}/(n+\sigma)! \quad .....(2)$$

$$a_n = \sum_{n_0+n_1+\ldots+n_m=n}\ \prod_{\mu=0}^{m}\binom{\rho_\mu-n_\mu-1}{n_\mu}\omega_\mu^{n_\mu} \quad .....(3)$$

Next, we define for $|z|_p = p^{-1/(p-1)-\theta}$,

$R_h(z,\omega,\rho) = R(z,\omega_0,\ldots,\omega_m,\rho_0+\delta_{ho},\ldots,\rho_m+\delta_{hm})$ $(h = 0, 1, \ldots, m)$

$A_{hk}(z,\omega,\rho) = A_k(z,\omega_0,\ldots,\omega_m,\rho_0+\delta_{ho},\ldots,\rho_m+\delta_{hm})$ $(h,k = 0, 1, \ldots, m)$

$D(z) = D(z,\omega,\rho) = \det\left(A_{hk}(z,\omega,\rho)\right)_{h,k=0,1,\ldots,m}$

where δ_{hk} denotes the familiar Kronecker symbol. Then we have the following algebraic identity (see e.g. p. 126 of Mahler (1932))

$$D(z) = \frac{\rho_0+\ldots+\rho_m}{\rho_0!\ldots\rho_m!}\prod_{k=0}^{m}\prod_{\substack{h=0\\ h\neq k}}^{m}(\omega_k-\omega_h)^{-\rho_h} \neq 0 \quad .....(4)$$

We shall now derive an estimate crucial to the proof of our theorem.

Lemma For z in $\mathbb{C}_p$ with $|z|_p = p^{-1/(p-1)-\theta}$, we have

$$|R(z,\omega,\rho)|_p \leq p^{-\theta\sigma}.$$

Proof From (3) we see that $|a_n|_p \leq 1$ and so $R(z) := R(z,\omega,\rho)$ is majorized by the p-adic exponential function e^z. Setting

$z = p^{1/(p-1)}w$ with $|w|_p < 1$, we know that $\exp(p^{1/(p-1)}w)$

considered as a function of w is a normal function (see p. 297 of Adams (1966)). Therefore, $R(p^{1/(p-1)}w)$ must also be a normal function of w. Since R (z) has a zero of order σ at the origin, then the normality gives (see p. 304 of Adams (1966))

$$|R(p^{1/(p-1)}w)|_p \leq p^{-\sigma\theta},$$

where $|w|_p = p^{-\theta}$ and the lemma follows.

RESULTS

We now proceed to prove our theorem. We first specialize the parameters in the last section as follows:

$0 = \omega_0 < \omega_1 < \ldots < \omega_m = \Omega$ are rational integers,

$\rho_0 = \rho_1 = \ldots = \rho_m = \rho$ are natural numbers.

Let

$$M_k = \prod_{\substack{j=0 \\ j \neq k}}^{m} |\omega_k - \omega_j|, \quad M = \underset{k=0,\ldots,m}{\text{L.C.M.}} M_k,$$

$$R_h(z) = R_h(z, \omega, \rho)$$

$$N = \underset{\substack{j,k=0,1,\ldots,m \\ j \neq k}}{\text{L.C.M.}} (\omega_k - \omega_j),$$

$$A_{hk}(z) = A_{hk}(z, \omega, \rho)$$

Take $z = p^v a/b$ to be rational with natural v satisfying $v > 1/(p-1)$, a rational integral, b natural with g.c.d. (a,p) = g.c.d. $(b,p) = 1$. Let

$$-v = -1/(p-1) - \theta, \quad \text{i.e.} \quad \theta = v - 1/(p-1).$$

For $h,k = 0, 1 \ldots, m$, put

$$a_{hk}(z) = b^\rho M^\rho N^{\rho+1} \rho!\ A_{hk}(z).$$

Then from the explicit formula (1) of $A_{hk}(z)$, we see that $a_{hk}(z)$ is a polynomial in z with rational integral coefficients and

$$a_{hk} := a_{hk}(p^v a/b) = b^\rho M^\rho N^{\rho+1} \rho! A_{hk}(p^v a/b)$$

is rational integral. Put also

$$r_h(z) = b^\rho M^\rho N^{\rho+1} \rho! R_h(z) \quad (h=0, 1 \ldots, m)$$

so that

$$r_h := r_h(p^v a/b) = \sum_{k=0}^{m} a_{hk} \exp(\omega_k p^v a/b)$$

From the lemma with $|z|_p = p^{-v} = p^{-1/(p-1)-\theta}$, we have

$$|R_h(z)|_p \leq p^{-(m+1)\rho\theta} \qquad (h=0, 1, \ldots, m)$$

and so using $|\rho!|_p \leq \rho p^{1-\rho/(p-1)}$ (see p. 187 of Bundschuh and Wallisser (1979)), we get

$$|r_h|_p \leq \rho p^{1-\rho/(p-1)-(m+1)\theta\rho}$$
$$= \rho p^{1-(m+1)\rho v + m\rho/(p-1)} \quad (h=0, 1 \ldots, m).$$

Let q_0 (≥ 1), $q_1, \ldots, q_m$ be m+1 arbitrary rational integers. Let

$$E^* = \max_{k=0,1,\ldots,m} \left| q_0 \exp(\omega_k p^v a/b) - q_k \right|_p = \max_{k=1,2,\ldots,m} \left| q_0 \exp(\omega_k p^v a/b) - q_k \right|_p$$

(since $\omega_0 = 0$)

and

$$E_k = q_0 \exp(\omega_k p^v a/b) - q_k \quad (k = 0, 1 \ldots, m).$$

Since the numbers $\exp(\omega_1 p^v a/b), \ldots, \exp(\omega_m p^v a/b)$ are transcendental (see Mahler (1932)), then $E^* > 0$.

Our aim now is to estimate E^* from below. First, we note from (4) that the determinant

$$\det (a_{hk})_{h,k=0,1,\ldots,m} \neq 0$$

and since the rational integers $q_0, q_1, \ldots, q_m$ do not all vanish, then there exists a suffix h such that

$$\sum_{k=0}^{m} a_{hk} q_k \neq 0$$

Now we observe that all parameters involved are rational numbers. Therefore, the universal algebraic identities (1), (2), (3) in the classical case yield (see pp. 202-204 of Mahler (1967))

$$A_{hk}(z) = \sum_{j=0}^{\rho} A_{hk}^{(j)} z^j / j!$$

with

$$\left|A_{hk}^{(j)}\right| \leq M_{\kappa}^{-\rho} m^{-m\rho}(m+1)^{(m+1)\rho} = C, \text{ say,}$$

so that

$$\left|A_{hk}\left(p^{v}a/b\right)\right| \leq C \sum_{j=0}^{\rho} \left|p^{v}a/b\right|^{j}/j!$$
$$< C(c+1)\left(1+\left|p^{v}a/b\right|\right).$$

Thus

$$| a_{hk} | = | a_{hk}(p^{v}a/b) |$$
$$= | b^{\rho} M^{\rho}N^{\rho+1} \rho! A_{hk} (p^{v}a/b) |$$
$$< Cb^{\rho} M^{\rho}N^{\rho+1} \rho! (\rho+1) (1+| p^{v}a/b |)$$
$$< 2b^{\rho} (13\rho m^{\Omega}e^{6\Omega})^{\rho} (\rho+1) (1+| p^{v}a/b |^{\rho})$$

(see p. 208 of Mahler (1967)). Consequently, we get for such h

$$1 \leq \left| \sum_{k=0}^{m} a_{hk} q_k \right| < S,$$

Where S = S (c,W,q,m,v,a,b) is as defined in the statement of the theorem and so

$$\left| \sum_{k=0}^{m} a_{hk} q_k \right|_p \geq \left| \sum_{k=0}^{m} a_{hk} q_k \right|^{-1} > 1/S .$$

With this value of h, put

$$Q = q_0^{-1} \sum_{k=0}^{m} a_{hk} q_k , E = q_0^{-1} \sum_{k=0}^{m} a_{hk} E_k .$$

Then

$$r_h = \sum_{k=0}^{m} a_{hk}\left(q_k/q_0 + E_k/q_0\right) = Q + E.$$

Now

$$|Q|_p = |q_0|_p^{-1} \left| \sum_{k=0}^{m} a_{hk} q_k \right|_p > |q_0|_p^{-1} S^{-1}$$

and

$$|E|_p \leq E^{*} \max_k \left|a_{hk} q_0^{-1}\right|_p \leq E^{*} |q_0|_p^{-1} .$$

If we have

$$\max_k |r_h|_p \leq |q_0|_p^{-1} S^{-1} (< |Q|_p) ,$$

then the strong triangle inequality yields

$$| E |_p = | Q |_p > 1/S \, | q_0 |_p,$$

and so

$$E^{*} \geq | E q_0 |_p > 1/S$$

and the theorem follows.

DISCUSSION

We deduce from our theorem a more pleasant looking result.

Corollary Let all notation be as set out in the theorem. Then there exist two positive constants K_1, K_2 depending only on p,m,a,b,Ω such that if

$$p^{v} \geq K_1 (\log q)^{1/m}$$

then

$$\max_{k=1,2,\ldots,m} \left| q_0 \exp\left(\omega_k p^{v} a/b\right) - q_k \right|_p > \exp\left(-K_2 v p^{mv}\right)$$

Proof The principal condition of the theorem is equivalent to

$$q^{-1} \geq (2 (m+1)p \, |q_0|_p) (\rho^{\rho+1}(\rho+1)) (13bm^{\Omega}e^{6\Omega}p^{m/(p-1)})^{\rho}$$
$$\times p^{-(m+1)v\rho} (1+| p^{v}a/b |^{\rho}),$$

which is implied by

$$q^{-1} \geq f(\rho) \qquad (5)$$

Where $f(x) = B^{x}_{1}\, x^{x}\, p^{-mvx}$ with

$$B_1 = B_1(p,m,a,b,\Omega)$$
$$= 52\,(m+1)\,bm^{\Omega}e^{6\Omega}p^{1+m/(p-1)}\,(1+|a/b|).$$

It is necessary then to have

$$q^{-1} \geq \min_{x>0} f(x) = \exp(-p^{mv}/eB_1)$$

i.e.

$$p^{v} \geq K_1 (\log q)^{1/m} \qquad (6)$$

(The possibility of $q = 1$ creates no difficulty for then the corollary is easily checked and for further discussion, we rule out this trivial case).

Also, if the condition (6) is satisfied, then since the minimum of $f(x)$ occurs at $x = x_0 = p^{mv}/eB_1$, which can certainly be made greater than or equal to 1 by enlarging K_1, we can find a positive integer $\rho \leq x_0$ such that (5) holds. Hence, all we need is (6) and this provides the estimate

$$E^* \geq B^{\rho}_{2}\, q^{-1}\, \rho^{-\rho}\, p^{-v\rho},$$

where $B_2 = B_1 p^{-(1+m/(p-1))}$, which using the value of ρ ($\leq x_0$) so chosen gives

$$E^* \geq \exp(-K_2\, v\, p^{mv})$$

We conclude this paper with some remarks.

(a) The condition (6) in the corollary is an improvement over the corresponding condition of Bundschuh and Wallisser (1979) which looks something like $K_3 \log q$ but the estimate for E^* above is a little worse; the corresponding one in Bundschuh and Wallisser is something like $\exp(-K_4 p^{v})$.

(b) There are also other methods yielding good lower bounds for E^*. For example, p-adic Baker theory (see van der Poorten (1977)) but the results there contain errors.

LITERATURE CITED

Adams, W.W. 1966. Transcendental numbers in the p-adic domain. Amer. J. math. 88 : 279-308.

Bundschuh, P. and R. Wallisser. 1979. Untere Schranken fur Polynome in Werten der p-adischen Exponentialfunktion. Math. Ann. 244 : 185-191.

Durand, A. 1980. Simultaneous diophantine approximations and Hermite's method. Bull. Austral. Math. Soc. 21 : 463-470.

Hermite, Ch. 1873. Oeuvres, t. III : 151-180.

LeVeque, W.J. 1956. Topics in Number Theory. Addison-Wesley, Reading-London.

Mahler, K. 1932. Zur Approximation der Exponentialfunktion und des Logarithmus, Tiel I, II. J. reine angew. Math. 166 : 118-150.

Mahler, K. 1932. Ein Beweis der Transzendenz der p-adischen Exponentialfunktion. J. rein angew. Math. 169 : 61-66.

Mahler, K. 1967. Applications of some formulae by Hermite to the approximation of exponentials and logarithms. Math. Ann. 168 : 200-227.

Serre, J.P. 1965/66. Dépendance d'exponentielles p-adiques. Séminaire Delange-Pisot Poitou, 7e année, #15.

Van der Poorten, A.J. 1977. Linear forms in logarithms in the p-adic case, in Transcendence Theory : Advances and Applications, ed. by A. Baker and D.W. Masser, Academic Press, London-New York-San Francisco.

Waldschmidt, M. 1973. Propriétes arithmétiques des valeurs de fonctions méromorphes algébriquement indépendantes. Acta Arith. 23 : 19-88.