

THE p -ADIC GENERALIZATION OF THE THUE-SIEGEL-ROTH THEOREM

D. RIDOUT

1. It was proved recently by Roth† that if α is any real algebraic number, and $\kappa > 2$, then the inequality

$$\left| \alpha - \frac{h}{q} \right| < \frac{1}{q^\kappa}$$

has only a finite number of solutions in integers h and q , where $q > 0$ and $(h, q) = 1$. This remarkable result answered finally a question which had been only partially answered by the work of Thue and Siegel.

The question of approximating by the same rational number h/q to a real root ζ of an algebraic equation and to p -adic roots ζ_1, \dots, ζ_t of the same equation, corresponding to different primes p_1, \dots, p_t , was investigated by Mahler‡, and the object of the present paper is to obtain a result for this problem which bears the same relation to Roth's theorem as Mahler's result bears to the earlier Thue-Siegel theorem.

We recall§ that for any prime p the p -adic field R_p is the extension of the rational field R effected by means of the p -adic valuation of R , the p -adic valuation $|x|_p$ of $x = a/b$ in R being defined by

$$|a/b|_p = p^{\theta(b) - \theta(a)} \quad (ab \neq 0),$$

where $\theta(a)$, $\theta(b)$ are the exact powers of p dividing the integers a , b . The p -adic valuation extends to apply to the elements of R_p .

We shall prove:

THEOREM 1. *Suppose the equation*

$$a_0 x^n + a_1 x^{n-1} + \dots + a_n = 0, \quad (1)$$

where $n \geq 2$, has rational integral coefficients, and has a root ζ in the real field, a root ζ_1 in the p_1 -adic field, ..., a root ζ_t in the p_t -adic field, where p_1, \dots, p_t are distinct primes. Then, if $\kappa > 2$, the inequality

$$\min(1, |\zeta - h/q|) \prod_{\tau=1}^t \min(1, |h - q\zeta_\tau|_{p_\tau}) \leq (\max(|h|, |q|))^{-\kappa} \quad (2)$$

has at most a finite number of solutions in rational integers h , q with $(h, q) = 1$, $q > 0$.

It will be noted that the p -adic valuations relate to $|q\zeta_\tau - h|_{p_\tau}$ and not to $|\zeta_\tau - h/q|_{p_\tau}$, so that the p -adic valuations are not on quite the same

† *Mathematika*, 2 (1955), 1–20. This paper will be referred to as **R**.

‡ *Math. Annalen*, 107 (1933), 691–730.

§ See, for example, van der Waerden, *Moderne Algebra I* (New York, 1953), 235–243.

footing as the real valuation. The theorem would assert less with $|\zeta_\tau - h/q|_{p_\tau}$, since $|q|_{p_\tau} \leq 1$.

The following theorem, which is expressed entirely in rational terms, follows from Theorem 1 as in the work of Mahler†, and is almost equivalent to it:

THEOREM 2. *Let $F(x, y)$ be an irreducible binary form of degree $n \geq 3$ with rational integral coefficients. Let p_1, \dots, p_t be distinct primes, and let $G(h, q)$ denote the greatest power-product of p_1, \dots, p_t which divides $F(h, q)$. Then, if $\kappa > 2$, the inequality*

$$\left| \frac{F(h, q)}{G(h, q)} \right| < \left(\max(|h|, |q|) \right)^{n-\kappa} \quad (3)$$

has at most a finite number of solutions in rational integers h, q with $(h, q) = 1$.

In a further paper‡, Mahler made a number of deductions concerning binary forms from the work of the first paper. But for these deductions the value of the exponent obtained in the first paper was unimportant, and it appears that we are unable to make any improvements in these results.

2. We first remark that, in proving Theorem 1, we can suppose that $a_0 = 1$ in (1). For if $f(x)$ denotes the polynomial on the left of (1), we have

$$f(x) = a_0^{-n+1} g(a_0 x),$$

where $g(y)$ is a polynomial with rational integral coefficients and highest coefficient 1. The roots of $g(y) = 0$ corresponding to $\zeta, \zeta_1, \dots, \zeta_t$ are $a_0 \zeta, a_0 \zeta_1, \dots, a_0 \zeta_t$. If

$$\frac{h'}{q'} = \frac{a_0 h}{q}, \quad (h', q') = 1,$$

then

$$\min(1, |\zeta - h/q|) \geq |a_0|^{-1} \min(1, |a_0 \zeta - h'/q'|),$$

$$\min(1, |q \zeta_\tau - h|_{p_\tau}) \geq \min(1, |q' a_0 \zeta_\tau - h'|_{p_\tau}),$$

$$\max(|h|, |q|) \geq |a_0|^{-1} \max(|h'|, |q'|).$$

Hence, if $\kappa > \kappa' > 2$, the inequality (2) implies a similar inequality for h', q' and the roots of $g(y) = 0$, with exponent κ' in place of κ , provided $\max(|h|, |q|)$ is sufficiently large. Thus it suffices if the latter inequality has at most a finite number of solutions.

† *Loc. cit.*, Hilfsatz 5 and §18.

‡ *Math. Annalen*, 108 (1933), 37–55.

3. We follow the work of **R** without change up to the beginning of §5. At this point we change slightly the definition of Θ_m ; we define

$$\Theta_m(B; h_1/q_1, \dots, h_m/q_m; r_1, \dots, r_m) \quad (4)$$

to be the upper bound of the index $\theta(R)$ of a polynomial $R(x_1, \dots, x_m)$ at the point $(h_1/q_1, \dots, h_m/q_m)$, for all polynomials in the set

$$\mathcal{R}_m(B; r_1, \dots, r_m).$$

Thus Θ_m as now defined depends on h_1, \dots, h_m , whereas the corresponding definition in **R** involved taking the upper bound over h_1, \dots, h_m .

The necessity for this change arises from the fact that the degree of precision of a rational approximation h/q in the present work is related to $\max(|h|, |q|)$ and not just to q . The main effect is that the choice of r_1, \dots, r_m at a later stage is now made to ensure that the numbers $\{\max(|h_j|, |q_j|)\}^{r_j}$ are of about the same magnitude, these numbers playing the part previously played by $q_j^{r_j}$.

We continue to follow the work of **R**, up to Lemma 9, with some changes of notation consequent upon the modified definition. The changes are slight, for the operation of taking the upper bound over h_1, \dots, h_m in **R** was a matter of convenience and not of principle. None of the arguments involved the consideration of more than one point at a time.

It is convenient to write

$$|h, q| = \max(|h|, |q|).$$

The assertion of Lemma 5 of **R** now takes the form:

$$\Theta_1(B; h_1/q_1; r_1) \leq \frac{\log B}{r_1 \log |h_1, q_1|}, \quad (5)$$

the proof being the same except for the further inequality $|h_1|^{\theta r_1} \leq B$, obtained by considering the coefficient of the lowest term in $R(x_1)$ as well as the coefficient of the highest term.

Lemma 6 of **R** requires only a change of notation, in that $\Theta_p, \Theta_1, \Theta_{p-1}$ now have reference respectively to $h_1/q_1, \dots, h_p/q_p$, to h_p/q_p , and to $h_1/q_1, \dots, h_{p-1}/q_{p-1}$. The proof is unchanged, since these are the points at which the indices are taken for the polynomials in p variables, 1 variable and $p-1$ variables, respectively.

Lemma 7 of **R** requires only a similar change of notation, except that the condition $r_j \log q_j \geq r_1 \log q_1$ in (22) of **R** is now replaced by

$$r_j \log |h_j, q_j| \geq r_1 \log |h_1, q_1|. \quad (6)$$

The condition on q_1 in (21) of **R** remains unchanged.

Lemma 8 of **R** has no reference to polynomials and requires no modification.

4. We come now to Lemma 9, the principal lemma of **R**, and this will be restated, with the necessary modifications, as Lemma 1 below. Let $f(x)$ be the polynomial in (1), with $a_0 = 1$. Let

$$A = \max(1, |a_1|, \dots, |a_n|). \quad (7)$$

We shall be concerned with one set of values of

$$m, \delta, q_1, h_1, \dots, q_m, h_m, r_1, \dots, r_m,$$

which will be chosen later in the order just indicated. The choice will be made to satisfy the conditions:

$$0 < \delta < m^{-1}, \quad (8)$$

$$10^m \delta^{(1/2)^m} + 2(1 + 3\delta)nm^{1/2} < \frac{1}{2}m, \quad (9)$$

$$r_m > 10\delta^{-1}, \quad r_{j-1}/r_j > \delta^{-1} \quad (j = 2, \dots, m), \quad (10)$$

$$\delta^2 \log q_1 > 2m + 1 + 2m \log(2 + A), \quad (11)$$

$$r_j \log |h_j, q_j| \geq r_1 \log |h_1, q_1|. \quad (12)$$

These conditions are (29)–(33) of **R**, with slight changes in the last two. Define $\lambda, \gamma, \eta, B_1$ as in **R** by

$$\lambda = 4(1 + 3\delta)nm^{1/2}, \quad (13)$$

$$\gamma = \frac{1}{2}(m - \lambda), \quad (14)$$

$$\eta = 10^m \delta^{(1/2)^m}, \quad (15)$$

$$B_1 = [q_1^{\delta r_1}]. \quad (16)$$

We note, as in **R**, that (9) is equivalent to

$$\eta < \gamma, \quad (17)$$

that B_1 is large, and that $q_1^{\frac{1}{2}\delta r_1} < B_1$.

LEMMA 1. *Let $(h_j, q_j) = 1$ for $j = 1, \dots, m$, and suppose that the conditions (8)–(12) are satisfied. Then there exists a polynomial $Q(x_1, \dots, x_m)$ with integral coefficients, of degree at most r_j in x_j for $j = 1, \dots, m$, such that*

(i) $Q_{i_1, \dots, i_m}(x, \dots, x)$ is divisible by $f(x)$ for all non-negative integers i_1, \dots, i_m satisfying

$$\frac{i_1}{r_1} + \dots + \frac{i_m}{r_m} < \gamma - \eta; \quad (18)$$

(ii) $Q(h_1/q_1, \dots, h_m/q_m) \neq 0$;

(iii) for any non-negative integers i_1, \dots, i_m , the coefficients of the polynomial $Q_{i_1, \dots, i_m}(x_1, \dots, x_m)$ have absolute values at most $B_1^{1+2\delta}$.

Proof. We follow the proof of Lemma 9 of **R** with slight modifications. We consider the same class of polynomials $W(x_1, \dots, x_m)$ as there, and deduce the existence of a polynomial $W^* = W' - W''$ such that

$$W_{j_1, \dots, j_m}^*(x, \dots, x)$$

is divisible by $f(x)$ for all j_1, \dots, j_m satisfying

$$0 \leq j_1 \leq r_1, \dots, 0 \leq j_m \leq r_m, \quad \frac{j_1}{r_1} + \dots + \frac{j_m}{r_m} \leq \gamma. \quad (19)$$

The coefficients in W^* are rational integers, not all 0, having absolute values at most B_1 .

The polynomial $W^*(x_1, \dots, x_m)$ belongs to the class $\mathcal{R}_m(q_1^{r_1}; r_1, \dots, r_m)$, and therefore by Lemma 7 of **R** its index at the point $(h_1/q_1, \dots, h_m/q_m)$ relative to r_1, \dots, r_m is less than η , defined in (15). Hence W^* possesses some derivative

$$Q(x_1, \dots, x_m) = \frac{1}{k_1! \dots k_m!} \left(\frac{\partial}{\partial x_1} \right)^{k_1} \dots \left(\frac{\partial}{\partial x_m} \right)^{k_m} W^*, \quad (20)$$

with

$$\frac{k_1}{r_1} + \dots + \frac{k_m}{r_m} < \eta, \quad (21)$$

such that $Q(h_1/q_1, \dots, h_m/q_m) \neq 0$.

Suppose i_1, \dots, i_m satisfy (18). Then Q_{i_1, \dots, i_m} is a constant multiple of W_{j_1, \dots, j_m}^* , where $j_1 = i_1 + k_1$, etc. By (21), j_1, \dots, j_m satisfy the last condition of (19), and therefore $W_{j_1, \dots, j_m}^*(x, \dots, x)$ is divisible by $f(x)$, being identically zero if $j_\nu > r_\nu$ for any ν . Hence the polynomial Q has the properties (i) and (ii). It is easily deduced, as in **R**, from the fact that W^* has coefficients of absolute value at most B_1 , that Q also has the property (iii).

5. We can now prove the following lemma, from which Theorem 1 will be deduced.

LEMMA 2. Let $\Gamma_0, \Gamma_1, \dots, \Gamma_t$ be non-negative real numbers satisfying

$$\Gamma_0 + \Gamma_1 + \dots + \Gamma_t = 1. \quad (22)$$

Then, if $\kappa > 2$, the $t+1$ simultaneous inequalities

$$\min(1, |\zeta - h/q|) \leq |h, q|^{-\kappa\Gamma_0}, \quad (23)$$

$$\min(1, |q\zeta_\tau - h|_{p_\tau}) \leq |h, q|^{-\kappa\Gamma_\tau} \quad (\tau = 1, \dots, t), \quad (24)$$

have at most a finite number of solutions in integers h, q satisfying $(h, q) = 1$.

It will be observed that the inequalities (23), (24) are significant only in so far as the corresponding exponent Γ is positive. Thus the lemma

covers three types of approximation: real approximation when

$$\Gamma_1 = \dots = \Gamma_t = 0 \quad (\text{Roth's result}),$$

p -adic approximation when $\Gamma_0 = 0$, and mixed approximation.

Proof. Suppose there are infinitely many solutions. First choose m so that $m > 4nm^{1/2}$ and

$$\frac{2m}{m-4nm^{1/2}} < \kappa,$$

as is possible since $\kappa > 2$. Next choose $\delta > 0$ so small that (8) and (9) are satisfied, and

$$\frac{2m(1+5\delta)}{m-4(1+3\delta)nm^{1/2}-2\eta} < \kappa.$$

This is equivalent to

$$m(1+5\delta) < \kappa(\gamma-\eta), \quad (25)$$

by (13) and (14).

Now choose a solution h_1, q_1 of the inequalities, with $(h_1, q_1) = 1$, such that q_1 satisfies (11). Then choose further solutions $h_2, q_2, \dots, h_m, q_m$, all with $(h_j, q_j) = 1$, to satisfy

$$\frac{\log q_j}{\log |h_{j-1}, q_{j-1}|} > \frac{2}{\delta} \quad (j = 2, \dots, m). \quad (26)$$

Take r_1 to be an integer satisfying

$$r_1 > \frac{10 \log |h_m, q_m|}{\delta \log q_1}, \quad (27)$$

and define r_2, \dots, r_m by

$$\frac{r_1 \log |h_1, q_1|}{\log |h_j, q_j|} \leq r_j < 1 + \frac{r_1 \log |h_1, q_1|}{\log |h_j, q_j|}. \quad (28)$$

Then (12) is satisfied. Also

$$\frac{r_j \log |h_j, q_j|}{r_1 \log |h_1, q_1|} < 1 + \frac{\log |h_j, q_j|}{r_1 \log |h_1, q_1|} < 1 + \frac{1}{10} \delta \quad (29)$$

by (27). The conditions (10) are satisfied, since

$$r_m \geq \frac{r_1 \log |h_1, q_1|}{\log |h_m, q_m|} \geq \frac{r_1 \log q_1}{\log |h_m, q_m|} > 10\delta^{-1}$$

and

$$\begin{aligned} \frac{r_{j-1}}{r_j} &> (1 + \frac{1}{10} \delta)^{-1} \frac{\log |h_j, q_j|}{\log |h_{j-1}, q_{j-1}|} \\ &> 2\delta^{-1} (1 + 10\delta)^{-1} > \delta^{-1}, \end{aligned}$$

for $j = 2, \dots, m$.

Since the conditions (8)–(12) are all satisfied, Lemma 1 gives the existence of a polynomial $Q(x_1, \dots, x_m)$ with the properties (i), (ii), (iii). We consider the rational integer Q defined by

$$Q = q_1^{r_1} \dots q_m^{r_m} Q(h_1/q_1, \dots, h_m/q_m), \quad (30)$$

which is not 0 by (ii). By an obvious property of p -adic valuations, we have

$$|Q| \prod_{\tau=1}^t |Q|_p \geq 1. \quad (31)$$

By the Taylor expansion of a polynomial, we have, for any α ,

$$Q = q_1^{r_1} \dots q_m^{r_m} \sum_{i_1=0}^{r_1} \dots \sum_{i_m=0}^{r_m} Q_{i_1, \dots, i_m}(\alpha, \dots, \alpha) (h_1/q_1 - \alpha)^{i_1} \dots (h_m/q_m - \alpha)^{i_m}. \quad (32)$$

We first use this to obtain an upper bound for $|Q|$. Taking $\alpha = \zeta$, we observe that by (i) of Lemma 1, the terms for which i_1, \dots, i_m satisfy (18) all vanish. In every other term we have, assuming $\Gamma_0 > 0$ and $|h_1, q_1| > 1$,

$$\begin{aligned} |h_1/q_1 - \zeta|^{i_1} \dots |h_m/q_m - \zeta|^{i_m} &\leq (|h_1, q_1|^{i_1} \dots |h_m, q_m|^{i_m})^{-\kappa\Gamma_0} \\ &\leq |h_1, q_1|^{-r_1(\gamma-\eta)\kappa\Gamma_0}, \end{aligned}$$

by (12). By (iii) of Lemma 1 and the well-known inequality $|\zeta| \leq 1 + A$, we have

$$\begin{aligned} |Q_{i_1, \dots, i_m}(\zeta, \dots, \zeta)| &\leq 2^{2mr_1} B_1^{1+2\delta} (1 + |\zeta|)^{r_1 + \dots + r_m} \leq 2^{2mr_1} B_1^{1+2\delta} (2 + A)^{mr_1} \\ &< B_1^{1+3\delta}, \end{aligned}$$

by (11). Hence

$$\begin{aligned} |Q| &\leq q_1^{r_1} \dots q_m^{r_m} (r_1 + 1) \dots (r_m + 1) B_1^{1+3\delta} |h_1, q_1|^{-r_1(\gamma-\eta)\kappa\Gamma_0} \\ &< |h_1, q_1|^{r_1 m(1+\delta) - r_1(\gamma-\eta)\kappa\Gamma_0} B_1^{1+4\delta}, \end{aligned}$$

on using (29). By the definition of B_1 , this implies

$$|Q| < |h_1, q_1|^E,$$

where

$$E = r_1 \{m(1+\delta) + \delta(1+4\delta) - (\gamma-\eta)\kappa\Gamma_0\}.$$

This estimate for $|Q|$ remains valid if $\Gamma_0 = 0$. For, taking $\alpha = 0$ in (32), we have

$$\begin{aligned} |Q| &\leq 2^{2mr_1} B_1^{1+2\delta} \sum_{i_1=0}^{r_1} \dots \sum_{i_m=0}^{r_m} |h_1^{i_1} \dots h_m^{i_m} q_1^{r_1-i_1} \dots q_m^{r_m-i_m}| \\ &\leq 2^{2mr_1} B_1^{1+2\delta} (r_1 + 1)^m |h_1, q_1|^{r_1} \dots |h_m, q_m|^{r_m} \\ &\leq B_1^{1+4\delta} |h_1, q_1|^{r_1 m(1+\delta)}, \end{aligned}$$

whence the same result as before.

We now estimate $|Q|_{p_\tau}$ in a similar manner, supposing first $\Gamma_\tau > 0$ and $|h_1, q_1| > 1$, taking $\alpha = \zeta_\tau$ in (32), and calculating in the field R_{p_τ} . The terms for which i_1, \dots, i_m satisfy (18) again vanish by (i) of Lemma 1. In every other term we have

$$|h_1 - q_1 \zeta_\tau|_{p_\tau}^{i_1} \dots |h_m - q_m \zeta_\tau|_{p_\tau}^{i_m} \leq (|h_1, q_1|^{i_1} \dots |h_m, q_m|^{i_m})^{-\kappa \Gamma_\tau} \\ \leq |h_1, q_1|^{-r_1(\gamma - \eta)\kappa \Gamma_\tau}.$$

We also have

$$|q_1^{r_1 - i_1} \dots q_m^{r_m - i_m}|_{p_\tau} \leq 1,$$

since the product is a non-zero rational integer. Since $Q_{i_1, \dots, i_m}(\alpha, \dots, \alpha)$ is a polynomial with rational integral coefficients, of degree not exceeding mr_1 , we have

$$|Q_{i_1, \dots, i_m}(\zeta_\tau, \dots, \zeta_\tau)|_{p_\tau} \leq \{\max(1, |\zeta_\tau|_{p_\tau})\}^{mr_1},$$

by the maximum rule for p -adic valuations. Hence

$$|Q|_{p_\tau} \leq |h_1, q_1|^{-r_1(\kappa - \eta)\kappa \Gamma_\tau} \{\max(1, |\zeta_\tau|_{p_\tau})\}^{mr_1}.$$

This remains true if $\Gamma_\tau = 0$, since Q is a rational integer and the right-hand side is then at least 1.

Using the estimates in (31), and noting that†

$$\prod_{\tau=1}^t \max(1, |\zeta_\tau|_{p_\tau}) \leq A,$$

we obtain

$$1 \leq A^{mr_1} |h_1, q_1|^{E'},$$

where

$$E' = r_1\{m(1 + \delta) + \delta(1 + 4\delta) - (\gamma - \eta)\kappa\},$$

by (22). Since $A^m < |h_1, q_1|^{\delta^2}$ by (11), we obtain

$$m(1 + \delta) + \delta(1 + 5\delta) > (\gamma - \eta)\kappa,$$

contrary to (25). This contradiction proves the lemma.

6. *Proof of Theorem 1.* Suppose the inequality (2) has infinitely many solutions in integers h, q with $(h, q) = 1$, $q > 0$. For any solution, we can write

$$\min(1, |\zeta - h/q|) = |h, q|^{-\kappa \gamma_0},$$

$$\min(1, |q \zeta_\tau - h|_{p_\tau}) = |h, q|^{-\kappa \gamma_\tau} \quad (\tau = 1, \dots, t),$$

where $\gamma_0, \gamma_1, \dots, \gamma_t$ are non-negative and

$$\gamma_0 + \gamma_1 + \dots + \gamma_t \geq 1.$$

† Mahler, *loc. cit.*, 701.

Choose κ' so that $2 < \kappa' < \kappa$. Choose a positive integer N to satisfy

$$N\left(\frac{\kappa}{\kappa'} - 1\right) > t + 1.$$

Then

$$\left[N \frac{\kappa}{\kappa'} \gamma_0\right] + \left[N \frac{\kappa}{\kappa'} \gamma_1\right] + \dots + \left[N \frac{\kappa}{\kappa'} \gamma_t\right] > N \frac{\kappa}{\kappa'} - (t + 1) > N.$$

Hence there exist, for each solution h, q , non-negative integers f_0, f_1, \dots, f_t such that

$$f_\tau \leq \left[N \frac{\kappa}{\kappa'} \gamma_\tau\right] \quad (\tau = 0, \dots, t)$$

and

$$f_0 + f_1 + \dots + f_t = N.$$

We have

$$\min(1, |\zeta - h/q|) \leq |h, q|^{-\kappa' f_0/N},$$

$$\min(1, |q\zeta_\tau - h|_{p_\tau}) \leq |h, q|^{-\kappa' f_\tau/N}$$

for $\tau = 1, \dots, t$.

There are only a bounded number (depending on N) of possibilities for f_0, \dots, f_t . Hence some set of these integers must occur for an infinity of solutions h/q of (2). For this set, supposing $|h, q| > 1$, the hypotheses of Lemma 2 are satisfied when κ is replaced by κ' and when we take

$$\Gamma_\tau = f_\tau/N \quad (\tau = 0, 1, \dots, t).$$

Thus we have a contradiction, and this proves Theorem 1.

Department of Mathematics,
University College,
London.

(Received 1st October, 1957.)