On the other hand, by (22),

$$\begin{aligned}|P(\boldsymbol{x}_{m+1})L(\boldsymbol{x}_m)-P(\boldsymbol{x}_m)L(\boldsymbol{x}_{m+1})| &> (\tfrac{1}{2}-\tfrac{32}{9}C_2)X_m^{-1}L_{m-1}^{-1}L_m-\tfrac{4}{3}C_2X_mL_m\\ &> (\tfrac{3}{8}-\tfrac{8}{3}C_2)X_mL_m-\tfrac{4}{3}C_2X_mL_m\\ &= (\tfrac{3}{8}-4C_2)X_mL_m.\end{aligned}$$

We have $\frac{8}{3}C_2 < \frac{3}{8}-4C_2$ since $C_2 < 9/160$. Thus we deduce that

$$X_mL_m < X_nL_n.$$

But this is impossible, since it leads to an infinite sequence of values of n for which X_nL_n increases, whereas we know that $X_nL_n \to 0$ as $n \to \infty$ by (18).

In view of the remarks at the end of § 1, this contradiction proves the theorem.

Note added in proof. We have since extended the basic result of this paper to a general theorem on $n-1$ linear forms in n variables, the result of the present paper being the case $n = 3$ with the linear forms $P(\boldsymbol{x})$, $L(\boldsymbol{x})$. See a forthcoming paper *A theorem on linear forms* in this journal. The more general result does not, however, solve the problem investigated by Wirsing and mentioned in § 1.

References

[1] J. F. Koksma, *Diophantische Approximationen*, Ergebn. Math. IV, 4.

[2] Th. Schneider, *Einführung in die transzendenten Zahlen*, Berlin 1957.

[3] E. Wirsing, *Approximation mit algebraischen Zahlen beschränkten Grades*, Journ. Math. 206 (1960), pp. 67-77.

TRINITY COLLEGE, CAMBRIDGE, ENGLAND,
UNIVERSITY OF COLORADO, BOULDER, COLORADO

Reçu par la Rédaction le 31. 1. 1967

ACTA ARITHMETICA
XIII (1967)

On two theorems of Gelfond and some of their applications

by

A. Schinzel (Warszawa)

§ 1. Introduction. The theorems mentioned in the title are concerned with the ordinary and $\mathfrak{p}$-adic measure of irrationality of the ratio of two logarithms of algebraic numbers. A. O. Gelfond, having estimated this measure [9], [10] was able in 1940 to deduce [10] for two elements α, β of an algebraic number field R and a prime ideal $\mathfrak{p}$ of R the inequalities

$$G_0 = \log|\alpha^n-\beta^m| - \max\{n\log|\alpha|, m\log|\beta|\} > -\log^{3+\varepsilon}\max\{|n|, |m|\},$$

$$G_{\mathfrak{p}} = \operatorname{ord}_{\mathfrak{p}}(\alpha^n-\beta^m) < \log^{3+\varepsilon}\max\{|n|, |m|\},$$

provided $\log|\alpha|/\log|\beta|$ is irrational and $n > n_0(\varepsilon, \alpha, \beta)$ or $\alpha^u\beta^v \neq 1$ for all integer pairs $(u, v) \neq (0, 0)$, α, β are $\mathfrak{p}$-adic units and $n > n_{\mathfrak{p}}(\varepsilon, \alpha, \beta)$, respectively.

In his book [11] published first in 1952 Gelfond has improved the estimates for the measure of irrationality of $\log\alpha_2/\log\alpha_1$ in a manner which permits to replace exponent $3+\varepsilon$ by $2+\varepsilon$ in the inequality for G_0. The same new method works *mutatis mutandis* in the $\mathfrak{p}$-adic case. It has also the advantage of being applicable if $\log\alpha_2/\log\alpha_1$ is irrational but $\alpha_1^u\alpha_2^v = 1$ for some integer $(u, v) \neq (0, 0)$, while the earlier method failed in this case as pointed out by V. Jarnik [13]. Therefore, the estimation for G_0 is true not only if $\log|\alpha|/\log|\beta|$ is irrational but as originally asserted by Gelfond in [10] if $\alpha^n-\beta^m \neq 0$ and the case $|\alpha| = |\beta| = 1$, $\alpha^u\beta^v \neq 1$ for all integer pairs $(u, v) \neq (0, 0)$ is excepted.

The applications I have in view require estimates for G_0 and $G_{\mathfrak{p}}$ that are explicit, i.e. do not involve the unspecified functions n_0 and $n_{\mathfrak{p}}$. For the purpose of finding such estimates earlier Gelfond's method is much more suitable than the very involved method of 1952. Therefore in § 2 I reproduce the arguments of [9] and [10] with such modifications as to replace $\log^{3+\varepsilon}\max\{|n|, |m|\}$ by $C(\alpha, \beta)\big(\log\max\{|n|, |m|\}+C'(\alpha, \beta)\big)^3$ or $C(\alpha, \beta, \mathfrak{p})\big(\log\max\{|n|, |m|\}+C'(\alpha, \beta, \mathfrak{p})\big)^3$ in the inequality for G_0 or $G_{\mathfrak{p}}$, respectively. $C(\alpha, \beta)$, $C'(\alpha, \beta)$, $C(\alpha, \beta, \mathfrak{p})$, $C'(\alpha, \beta, \mathfrak{p})$ are constants written

out explicitly in Theorems 1 and 2. Moreover if $\log|\alpha|/\log|\beta|$ is rational I obtain

$$G_0 > -C(\alpha,\beta)\left(\log\max\{|n|,|m|\}+C'(\alpha,\beta)\right)^2.$$

This is the only result of the present paper which can be considered as an improvement of Gelfond's work of 1952. It is reformulated as Corollary 1 in terms of Diophantine approximation.

§ 3 is devoted to the study of linear recurrences of the second order. If the companion polynomial of such a recurrence $\{u_n\}$ has real roots, the order of magnitude of $|u_n|$ can be found easily. If the roots are not real, Thue-Siegel theorem implies that $\log|u_n|$ is of order n, it does not permit however to find for a given c a number $n_0(c)$ such that $|u_n| \neq c$ for $n > n_0(c)$. For special recurring sequences $n_0(c)$ was given explicitly by P. Chowla, S. Chowla, M. Dunton, D. J. Lewis [8], S. B. Townes [24] and A. Schinzel [21]. Theorems 3 and 4 contain explicit estimates for u_n which comprise all the above results. One of these estimates is applied next to the study of the equation $x^2-d=2^n$ (d negative), investigated by many authors (cf. H. Hasse [12]). J. Browkin and I conjectured [5] that for $d \neq 1-2^k, -23$ the equation has at most one solution in positive integers x, n. Townes has proved that this is the case for $d=-7y^2$ and R. Apéry [1] has proved that for $d \neq -7$ there exist at most two solutions. Theorem 5 shows that our original conjecture can be decided by a finite although large amount of computations and Theorem 6 generalizes this result to the equation $x^2-d=p^n$ (p prime). Finally, Theorems 7 and 8 contain estimates of the greatest prime factor of u_n denoted by $q(u_n)$.

§ 4 is concerned with the expression $x^r \pm P_1^{n_1}P_2^{n_2}\dots P_k^{n_k}$ where $r=2$ or 3 and $P_1,\dots,P_k$ are positive integers. I estimate the order of magnitude of this expression (Theorem 9) and for $k \leqslant 3$ and P_i suitably restricted its greatest prime factor (Theorem 10). As a Corollary 5 to Theorem 9 I obtain for any quadratic irrationality ξ and any basis of notation g an effective estimate for $\|\xi g^n\|$ which says a little more than Liouville's theorem. On the other hand, Theorem 10 permits to solve effectively all Diophantine equations of the form

$$q_1^{y_1}q_2^{y_2}\dots q_i^{y_i} \pm r_1^{z_1}r_2^{z_2}\dots r_j^{z_j} = s^x,$$

where $q_1,\dots,q_i,r_1,\dots,r_j$ are distinct primes and s is a positive integer, not divisible by 6 if the sign is lower. This result included in Corollary 6 generalizes the results of H. Rumsey, Jr. and E. C. Posner [20] and partly those of J. W. S. Cassels [7], who was first to use Gelfond's estimates in that connection.

§ 5 is devoted to the study of the greatest prime factor of a quadratic or cubic polynomial. K. Mahler [16] and T. Nagell [18], [19] proved that for binomials $Ax^2\pm1$, ±2, ±4 and $Ax^3\pm1$, ±3 the greatest prime factor exceeds $c\log\log x$, where c is a positive constant. These results are

improved (as to the value of c) in Theorem 12 and generalized to arbitrary quadratic and cubic binomials in Theorem 11. Next, the question is considered how small the greatest prime factor of an arbitrary polynomial $f(x)$ can be for a suitable x (Theorems 13-15). The proofs are given for the results in this direction I announced in Stockholm [22]. An open problem closes the paper.

The recent solution by A. N. Baker of the problem of three logarithms (Mathematika 13 (1966), pp. 204-216) would permit to generalize many results of this paper and to obtain the true order of magnitude of $\log|u_n|$ in Theorem 3. This, however, cannot be done without a certain amount of adaptation and may form an object of another work.

§ 2. Fundamental theorems

Notation. R is an algebraic number field of degree ν and of discriminant D. α, β are non-zero elements of R;

$$\alpha = \alpha''/\alpha', \qquad \beta = \beta''/\beta',$$

where $\alpha', \alpha'', \beta', \beta''$ are integers of R,

$$a = \log\max\left\{|eD|^{1/\nu^2}, \overline{|\alpha'\beta'|}, \overline{|\alpha'\beta''|}, \overline{|\alpha''\beta'|}, \overline{|\alpha''\beta''|}\right\},$$

where $\overline{|\gamma|}$ is the maximal absolute value of the conjugates of γ.

$\mathfrak{p}$ is a prime ideal of R with the norm p^e where p is a rational prime, $R_\mathfrak{p}$ is the $\mathfrak{p}$-adic completion of R,

$$\mu = \frac{\nu}{e\log p}, \qquad \varphi = \operatorname{ord}_\mathfrak{p} p.$$

R_0 is a field containing $|\alpha|$, $|\beta|$ of degree ν_0 and of discriminant D_0,

$$|\alpha| = \frac{\alpha_0''}{\alpha_0'}, \qquad |\beta| = \frac{\beta_0''}{\beta_0'},$$

where $\alpha_0', \alpha_0'', \beta_0', \beta_0''$ are integers of R_0;

$$a_0 = \log\max\left\{|eD_0|^{1/\nu_0^2}, \overline{|\alpha_0'\beta_0'|}, \overline{|\alpha_0'\beta_0''|}, \overline{|\alpha_0''\beta_0'|}, \overline{|\alpha_0''\beta_0''|}\right\},$$

$$a_1 = \max\left\{\frac{2\pi}{\nu}, a\right\}.$$

If $|\alpha| \neq 1$ or $|\beta| \neq 1$ and $|\alpha|^{u_0} = |\beta|^{v_0}$, $(u_0, v_0) = 1$ for some rational integers u_0, v_0, we set

$$a_2 = \begin{cases} \max\left\{\dfrac{2\pi}{\nu}, \dfrac{\log|eD|}{\nu^2}, \log\overline{\left|\alpha'^{|u_0|}\beta'^{|v_0|}\right|}, \log\overline{\left|\alpha''^{|u_0|}\beta''^{|v_0|}\right|}\right\} & \text{if} \quad u_0v_0 \leqslant 0, \\ \max\left\{\dfrac{2\pi}{\nu}, \dfrac{\log|eD|}{\nu^2}, \log\overline{\left|\alpha'^{|u_0|}\beta''^{|v_0|}\right|}, \log\overline{\left|\alpha''^{|u_0|}\beta'^{|v_0|}\right|}\right\} & \text{if} \quad u_0v_0 > 0. \end{cases}$$

m, n and n_1, n_2 are rational integers, $n_1 \neq 0$, $N = \max\{|m|, |n|\} > 0$, $H = \max\{|n_1|, |n_2|\}$.

THEOREM 1. *If α or β is a $\mathfrak{p}$-adic unit and $\alpha^n - \beta^m \neq 0$, then*

$$\operatorname{ord}_{\mathfrak{p}}(\alpha^n - \beta^m) < 10^6 \mu^7 \varrho^{-2} a^4 p^{40+4}(\log N + \varrho a p^{\varrho} + 2a^{-1})^3.$$

THEOREM 2. *If $\alpha^n - \beta^m \neq 0$ and we exclude the case $|\alpha| = |\beta| = 1$, α, β multiplicatively independent, then*

$$\log|\alpha^n - \beta^m| - \max\{n\log|\alpha|, m\log|\beta|\}$$

$$> \begin{cases} -10^5 \nu^5 a_1 (\log N + \nu)^2 \\ \quad \text{if } |\alpha| = |\beta| = 1 \text{ and } \alpha, \beta \text{ are multiplicatively dependent,} \\ -\max\{10^5 \nu^5 a_2^3 (\log N + \nu)^2, \nu_0 (2a_0 + 5)\} \\ \quad \text{if } |\alpha| \neq 1 \text{ or } |\beta| \neq 1 \text{ and } |\alpha|, |\beta| \text{ are multiplicatively dependent,} \\ -5 \cdot 10^6 \nu_0^7 a_0^4 (\log N + a_0 + 1 + a_0^{-1})^3 \\ \quad \text{if } |\alpha|, |\beta| \text{ are multiplicatively independent.} \end{cases}$$

LEMMA 1. *If $\gamma \neq 0$ is an arbitrary integer of R then*

$$\operatorname{ord}_{\mathfrak{p}} \gamma \leqslant \mu \log \overline{|\gamma|}, \tag{1}$$

$$\log|\gamma| \geqslant -(\nu - 1)\log \overline{|\gamma|}. \tag{2}$$

Proof. Let g be the norm of γ. Clearly

$$0 \leqslant \log|g| \leqslant \log|\gamma| + (\nu - 1)\log \overline{|\gamma|} \leqslant \nu \log \overline{|\gamma|},$$

whence (2) follows at once.

On the other hand, setting $\operatorname{ord}_{\mathfrak{p}} \gamma = \delta$ we have

$$(\operatorname{norm} \mathfrak{p})^{\delta} | \operatorname{norm} \gamma, \quad \text{i.e.} \quad p^{\varrho\delta} | g,$$

thus

$$\operatorname{ord}_{\mathfrak{p}} \gamma \leqslant \frac{1}{\varrho} \operatorname{ord}_p g \leqslant \frac{1}{\varrho} \cdot \frac{\log|g|}{\log p} \leqslant \frac{\nu}{\varrho \log p} \log \overline{|\gamma|},$$

which gives (1).

LEMMA 2. *If either α or β is not a root of unity and $\alpha^u = \beta^v$, where $|u| + |v| > 0$, then*

$$\frac{|u| + |v|}{(u, v)} \leqslant \nu a (2^{\nu+4} + 1).$$

Proof. If one of α, β is a root of unity, we have $u = 0$ or $v = 0$ which implies the assertion of the lemma. Thus it remains to consider the case, where neither α or β is a root of unity. Following [22] we denote

for any $\gamma \in R$ which is not 0 or a root of unity, by $e(\gamma, R)$ the greatest integer f such that

$$\gamma = w\delta^f, \quad \text{where } \delta \in R \text{ and } w \text{ is a root of unity.}$$

If γ is a root of unity we define $e(\gamma, R) = 0$. By Lemma 1 of [22] we have for any rational integer g

$$e(\gamma^g, R) = |g| e(\gamma, R),$$

hence

$$|u| e(\alpha, R) = e(\alpha^u, R) = e(\beta^v, R) = |v| e(\beta, R),$$

and

$$e(\alpha, R) \geqslant |v|/(u, v). \tag{3}$$

On the other hand, since $(\alpha\beta^{\pm 1})^v = \alpha^{v \pm u}$ we have

$$|v| e(\alpha\beta^{\pm 1}, R) = e(\alpha^{v \pm u}, R) = |v \pm u| e(\alpha, R), \tag{4}$$

where the sign is chosen so that $|v \pm u| = |u| + |v|$.

It follows from (3) and (4) that

$$\frac{|u| + |v|}{(u, v)} \leqslant \max\{e(\alpha\beta, R), e(\alpha\beta^{-1}, R)\}. \tag{5}$$

The estimation given in Lemma 1 of [22] for $e(\gamma, R)$ is not suitable for our purposes, however it is clear from the proof of that lemma and the remark 1 at the end of [22] that

$$e(\gamma, R) \leqslant \begin{cases} (2^{\nu+4} + 1)\log \overline{|\gamma|} & \text{if } \gamma \text{ is an integer of } R, \\ \nu \dfrac{\log \overline{|\gamma'|}}{\log 2} & \text{if } \gamma \text{ is not an integer of } R \text{ but } \gamma' \text{ and } \gamma\gamma' \text{ are.} \end{cases}$$

If $\alpha\beta$ is not an integer we apply this inequality with $\gamma' = \alpha'\beta'$ and obtain

$$e(\alpha\beta, R) \leqslant \nu \frac{a}{\log 2} < \nu a (2^{\nu+4} + 1).$$

If $\alpha\beta$ is an integer, we have

$$\log \overline{|\alpha\beta|} = \log \overline{\left|\frac{\alpha''\beta''}{\alpha'\beta'}\right|} \leqslant \log \overline{|\alpha''\beta''|} + \log \overline{|(\alpha'\beta')^{-1}|}.$$

However by Lemma 1

$$\log \overline{|(\alpha'\beta')^{-1}|} \leqslant (\nu - 1)\log \overline{|\alpha'\beta'|},$$

thus $\overline{|\alpha\beta|} \leqslant \nu a$ and we obtain again

$$e(\alpha\beta, R) \leqslant \nu a (2^{\nu+4} + 1). \tag{6}$$

Similarly

$$e(a\beta^{-1}, R) \leqslant \nu a(2^{\nu+4}+1) \tag{7}$$

and the lemma follows from (5), (6) and (7).

LEMMA 3. *Suppose the coefficients a_{ks} of the linear forms*

$$L_k = a_{k1}x_1 + \ldots + a_{kQ}x_Q, \quad 1 \leqslant k \leqslant P < Q$$

are integers of R and

$$\max_{k,s} |a_{ks}| \leqslant A. \tag{8}$$

Then there exists a solution of the system of equations $L_k = 0$ $(1 \leqslant k \leqslant P)$ in integers $x_1, \ldots, x_Q$ of R with

$$0 < \max_{1 \leqslant q \leqslant Q} |x_q| \leqslant C(CQA)^{P/(Q-P)},$$

where

$$C \leqslant \sqrt{\nu^{5\nu}|D|} \leqslant \exp \tfrac{1}{2}(5\nu \log \nu + \nu^2 a).$$

Proof. For $\nu = 1$ the lemma follows at once from Lemma 3, Chapter VI of [6]. Assume $\nu > 1$.

By Lemma 1 of [26], there exists in R an integral basis $w_1, w_2, \ldots, w_\nu$ such that

$$\sqrt{\prod_{i=1}^{\nu}\Big(\sum_{j=1}^{\nu}|w_i^{(j)}|^2\Big)} \leqslant 2\nu!\,\Gamma(1+\nu/2)\,\pi^{-\nu/2}\sqrt{|D|} \tag{9}$$

(the superscripts denote conjugates).

Clearly for all $i \leqslant \nu$

$$\sum_{j=1}^{\nu}|w_i^{(j)}|^2 \geqslant \nu\sqrt[\nu]{\prod_{j=1}^{\nu}|w_i^{(j)}|^2} \geqslant \nu. \tag{10}$$

Hence by (9)

$$\sqrt{\sum_{j=1}^{\nu}|w_i^{(j)}|^2} \leqslant 2\nu!\,\Gamma(1+\nu/2)\,\pi^{-\nu/2}\sqrt{|D|}\,\nu^{(1-\nu)/2}. \tag{11}$$

It follows from (8), (10), (11) and Schwartz's inequality that for all $h, r \leqslant \nu$, $k \leqslant P$, $s \leqslant Q$

$$\begin{aligned}\sqrt{\sum_{j=1}^{\nu}|w_h^{(j)}a_{ks}^{(j)}|^2} &\leqslant \sqrt{\sum_{j=1}^{\nu}|w_h^{(j)}|^2}\sqrt{\sum_{j=1}^{\nu}|a_{ks}^{(j)}|^2} \\ &\leqslant 2\nu!\,\Gamma(1+\nu/2)\,\nu^{(1-\nu)/2}\pi^{-\nu/2}\sqrt{|D|}\,A\sqrt{\sum_{j=1}^{\nu}|w_r^{(j)}|^2}.\end{aligned} \tag{12}$$

Set

$$w_h^{(j)}a_{ks}^{(j)} = \sum_{r=1}^{\nu} b_{hksr}w_r^{(j)},$$

where b_{hksr} are rational integers. By Cramer's formulae, Hadamard's inequality, (12) and (9) we have

$$\begin{aligned}|b_{hksr}| &= \left|\frac{1}{\det(w_r^{(j)})}\begin{vmatrix} w_1^{(1)} \ldots w_{r-1}^{(1)} & w_h^{(1)}a_{ks}^{(1)} & w_{r+1}^{(1)} & w_\nu^{(1)} \\ \cdots & \cdots & \cdots & \cdots \\ w_1^{(\nu)} \ldots w_{r-1}^{(\nu)} & w_h^{(\nu)}a_{ks}^{(\nu)} & w_{r+1}^{(\nu)} & w_\nu^{(\nu)} \end{vmatrix}\right| \\ &\leqslant \frac{1}{\sqrt{|D|}}\sqrt{\sum_{j=1}^{\nu}|w_h^{(j)}a_{ks}^{(j)}|^2\prod_{\substack{i=1\\ i\neq r}}^{\nu}\Big(\sum_{j=1}^{\nu}|w_i^{(j)}|^2\Big)} \\ &\leqslant 2\nu!\,\Gamma(1+\nu/2)\,\nu^{(1-\nu)/2}\pi^{-\nu/2}A\prod_{i=1}^{\nu}\Big(\sum_{j=1}^{\nu}|w_i^{(j)}|^2\Big) \\ &\leqslant 4(\nu!)^2\Gamma(1+\nu/2)^2\nu^{(1-\nu)/2}\pi^{-\nu}\sqrt{|D|}A = BA.\end{aligned}$$

Consider the system of equations

$$\sum_{r=1}^{\nu}\sum_{s=1}^{Q} b_{rksh}x_{sr} = 0, \quad 1 \leqslant k \leqslant P, \quad 1 \leqslant h \leqslant \nu. \tag{13}$$

The number of equations in this system is νP and the number of variables is $\nu Q > \nu P$. By Lemma 3, Chapter VI of [6], there exists a solution of (13) in rational integers x_{sr} such that

$$0 < \max_{s,r}|x_{sr}| \leqslant (\nu QBA)^{P/(Q-P)}. \tag{14}$$

Put

$$x_s = \sum_{r=1}^{\nu} x_{sr}w_r, \quad 1 \leqslant s \leqslant Q.$$

We have

$$|x_s| \leqslant \nu\max_r |x_{sr}|\,|w_r|,$$

hence by (11) and (14)

$$|x_s| \leqslant C(CQA)^{P/(Q-P)},$$

where

$$C = 4(\nu!)^2\Gamma(1+\nu/2)^2\,\nu^{(3-\nu)/2}\pi^{-\nu}\sqrt{|D|}.$$

Since for $\nu > 1$, $C < \sqrt{\nu^{5\nu}|D|}$, the lemma follows.

LEMMA 4. *Let $f(z)$ be a normal function on R_ν, s_0, r_1, s_1 be rational integers, $r_1 \geqslant 1$, $s_0 \geqslant 1$, $s_1 \geqslant 0$,*

$$\omega = \min_{\substack{0 \leqslant r < r_1 \\ 0 \leqslant s < s_0}} \operatorname{ord}_\nu f^{(s)}(pr). \tag{15}$$

Then

$$\operatorname{ord}_p f^{(s_1)}(pr_1) \geqslant \min\left\{\varphi(r_1 s_0 - s_1),\ -\varphi(s_0+s_1)\frac{\log pr_1}{\log p} + \omega\right\}$$

(*we assume* $\operatorname{ord}_p 0 = \infty$).

Proof. The lemma follows directly (apart from the case $s_0 = 1$ or $r_1 = 1$) from Lemma III of [10], by the substitution $y = r_2$ and a permutation of letters. The proof of that lemma although valid in principle contains a number of mistakes, therefore we reproduce it with the corrections and with some simplifications taken from [11], pp. 121-122.

Consider an interpolation polynomial $P(z)$ of degree $r_1 s_0 - 1$ defined by the conditions

$$P^{(s)}(pr) = f^{(s)}(pr), \quad 0 \leqslant r < r_s,\ 0 \leqslant s < s_0. \tag{16}$$

By Hermite's interpolation formula

$$P(z) = \sum_{r=0}^{r_1-1}\sum_{s=0}^{s_0-1}\sum_{h=0}^{s_0-s-1} f^{(s)}(pr) A_{rsh} Q_{rh}(z), \tag{17}$$

where

$$A_{rsh} = \frac{1}{s!(r_0-s-h-1)!}\cdot\frac{d^{r_0-s-h-1}}{dz^{r_0-s-h-1}}\left(\frac{(z-pr)^{s_0}}{Q(z)}\right)\Bigg|_{z=pr},$$

$$Q_{rh}(z) = (z-pr)^{-h-1}Q(z)$$

and

$$Q(z) = \prod_{r=0}^{r_1-1}(z-pr)^{s_0}.$$

Differentiating we obtain

$$A_{rsh} = \frac{(-1)^{s_0-s-1}}{s!}\cdot\frac{p^{-r_1 s_0+s+h+1}}{(r!(r_1-r-1)!)^{s_0}}\sum\prod_{k=0}^{r_1-1}\binom{s_0+h_k-1}{h_k}(r-k)^{-h_k},$$

where the summation is taken over all systems of non-negative integers $h_0, \ldots, h_{r_1-1}$ satisfying

$$h_0+h_1+\ldots+h_{r_1-1} = s_0-s-h-1, \quad h_r = 0.$$

Since $\operatorname{ord}_p s! < \varphi s$ and for $k \neq r$, $0 \leqslant k < r_1$,

$$\operatorname{ord}_p(r-k) \leqslant \operatorname{ord}_p r_1 < \varphi\frac{\log r_1}{\log p}$$

we get

$$\operatorname{ord}_p A_{rsh} \geqslant \varphi(-r_1 s_0+h+1) - s_0\operatorname{ord}_p(r!(r_1-r-1)!) - \varphi s_0\frac{\log r_1}{\log p}. \tag{18}$$

Similarly, differentiating $Q_{rh}(z)$ we obtain

$$Q_{rh}^{(s_1)}(pr_1) = s_1! p^{r_1 s_0-h-s_1-1}\frac{(r_1!)^{s_0}}{(r_1-r)^{h+1}}\sum\binom{s_0-h-1}{\sigma_r}(r_1-r)^{-\sigma_r}\prod_{\substack{k=0\\k\neq r}}^{r_1-1}\binom{s_0}{\sigma_k}(r_1-k)^{-\sigma_k},$$

where the summation is taken over all systems of non-negative integers $\sigma_0, \ldots, \sigma_{r_1-1}$ satisfying

$$\sigma_0+\sigma_1+\ldots+\sigma_{r_1-1} = s_1, \quad \sigma_r \leqslant s_0-h-1.$$

Hence

$$\operatorname{ord}_p Q_{rh}^{(s_1)}(pr_1) \geqslant \varphi(r_1 s_0-h-s_1-1)+s_0\operatorname{ord}_p(r_1!/(r_1-r))-\varphi s_1\frac{\log r_1}{\log p}. \tag{19}$$

It follows from (15), (17), (18) and (19) that

$$\operatorname{ord}_p P^{(s_1)}(pr_1) \geqslant -\varphi(s_0+s_1)\frac{\log pr_1}{\log p} + \omega. \tag{20}$$

On the other hand, by Newton's interpolation formula

$$P(z) = \sum_{r=0}^{r_1-1}\sum_{s=0}^{s_0-1} A_{rs}\big(z(z-p)(z-pr+p)\big)^{s_0}(z-pr)^s,$$

where

$$A_{rs} = \sum_{i=0}^{\infty} B_{rs}^{(i)}\frac{f^{(i)}(0)}{i!}$$

and $B_{rs}^{(i)}$ is the slope of x^i taken in the point

$$(\underbrace{0, p, \ldots, pr-p, 0, p, \ldots, pr-p, 0, p, \ldots, pr-p}_{s_0 \text{ times}}, \underbrace{pr, pr, \ldots, pr}_{s+1 \text{ times}}).$$

$B_{rs}^{(i)}$ is a rational integer and since by the definition of a normal function

$$\operatorname{ord}_p\frac{f^{(i)}(0)}{i!} \geqslant 0, \quad \lim_{i=\infty}\operatorname{ord}_p\frac{f^{(i)}(0)}{i!} = \infty,$$

A_{rs} is well defined, $\operatorname{ord}_p A_{rs} \geqslant 0$ and $P(z)$ is a normal function.

It follows that the function $F(z) = f(z) - P(z)$ is also normal and by (16)

$$F(z) = \big(z(z-p)\ldots(z-pr_1+p)\big)^{s_0}F_1(z)$$

where $F_1(z)$ is a normal function. Thus

$$\text{ord}_{\mathfrak{p}} F^{(s_1)}(pr_1) \geqslant \text{ord}_{\mathfrak{p}} \frac{d^{s_1}}{dz^{s_1}}\big(z(z-p)\dots(z-pr_1+p)\big)^{s_0}\big|_{z=pr_1} \tag{21}$$

$$\geqslant \varphi(r_1 s_0 - s_1).$$

Since $f^{(s_1)}(pr_1) = F^{(s_1)}(pr_1) + P^{(s_1)}(pr_1)$ the lemma follows from (20) and (21).

LEMMA 5. *If $\gamma \in R$, $\gamma \neq 1$, $\text{ord}_{\mathfrak{p}}(\gamma-1) > \varphi/(p-1)$ and η is the $\mathfrak{p}$-adic logarithm of γ, then $e(\eta z)$ is a normal function on $R_{\mathfrak{p}}$ which for rational integers z coincides with γ^z and*

$$\text{ord}_{\mathfrak{p}} \eta = \text{ord}_{\mathfrak{p}}(\gamma-1). \tag{22}$$

Remark. We write $e(z)$ instead of $\exp z$, reserving the notation $\exp z$ to its ordinary use.

Proof. By Theorem 3, Chapter VI of [4], we have

$$\text{ord}_{\mathfrak{p}} \eta > \varphi/(p-1). \tag{23}$$

Since for $k \geqslant 1$, $\text{ord}_{\mathfrak{p}} k! \leqslant \varphi \dfrac{k-1}{p-1}$, we get

$$\text{ord}_{\mathfrak{p}} \frac{\eta^k}{k!} \geqslant \text{ord}_{\mathfrak{p}} \eta + (k-1)\left(\text{ord}_{\mathfrak{p}} \eta - \frac{\varphi}{p-1}\right) \quad (k \geqslant 1) \tag{24}$$

and it follows that the function

$$e(\eta z) = \sum_{k=0}^{\infty} \frac{\eta^k}{k!} z^k$$

is normal.

Again by the quoted theorem, we have for rational integers z

$$e(\eta z) = \big(e(\eta)\big)^z = \gamma^z.$$

In particular, for $z = 1$, we get

$$\sum_{k=0}^{\infty} \frac{\eta^k}{k!} = \gamma; \qquad \eta + \sum_{k=2}^{\infty} \frac{\eta^k}{k!} = \gamma - 1.$$

Since by (23) and (24)

$$\text{ord}_{\mathfrak{p}} \sum_{k=2}^{\infty} \frac{\eta^k}{k!} > \text{ord}_{\mathfrak{p}} \eta$$

(22) follows.

LEMMA 6. *Let $\alpha_1, \alpha_2 \in R$, $\alpha_i = \alpha_i''/\alpha_i'$, where α_i', α_i'' are integers of R,*

$$b = \max\left\{\frac{\varphi}{\mu p}, \log\max\left\{\left|\overline{\alpha_1'\alpha_2'}\right|, \left|\overline{\alpha_1'\alpha_2''}\right|, \left|\overline{\alpha_2'\alpha_1''}\right|, \left|\overline{\alpha_1''\alpha_2''}\right|\right\}\right\}.$$

Suppose that $\alpha_1 \neq 1$, $\text{ord}_{\mathfrak{p}}(\alpha_2 - 1) \geqslant \text{ord}_{\mathfrak{p}}(\alpha_1 - 1) > \varphi/(p-1)$, η_i is the $\mathfrak{p}$-adic logarithm of α_i and η_2/η_1 is irrational.

If a positive integer q satisfies the inequality

$$q^2 - 27\mu\varphi^{-2} bpq(\mu \log 2Hq + \tfrac{2}{3}\,\text{ord}_{\mathfrak{p}}\eta_1 + \tfrac{2}{3}\mu + \tfrac{83}{81}\varphi) - 9\mu\varphi^{-1}\log C > 0, \tag{25}$$

where C is the constant of Lemma 3, then

$$\text{ord}_{\mathfrak{p}}\left(\frac{\eta_2}{\eta_1} - \frac{n_2}{n_1}\right) < \mu bp(q+1)^3.$$

Proof. Put

$$r_0 = \left[\frac{\varphi q}{9\mu bp}\right], \qquad s_0 = \left[\frac{3\mu bpq}{\varphi}\right]$$

and consider the following linear forms

$$L_{rs}([x_{q_1q_2}]) = \sum_{q_1=0}^{q}\sum_{q_2=0}^{q} x_{q_1q_2}(n_1q_1 + n_2q_2)^s (\alpha_1'\alpha_2')^{pqr} \alpha_1^{pq_1r} \alpha_2^{pq_2r}$$

$$(0 \leqslant r < r_0,\ 0 \leqslant s < s_0).$$

Since $\mu\varphi^{-1}bp \geqslant 1$ and by (25) $q \geqslant 9\mu\varphi^{-1}bp$ we have $r_0 \geqslant 1$, $s_0 \geqslant 1$. Since

$$(\alpha_1'\alpha_2')^q \alpha_1^{q_1}\alpha_2^{q_2} = (\alpha_1'\alpha_2')^{q-\max\{q_1,q_2\}} (\alpha_1''\alpha_2'')^{\min\{q_1,q_2\}} \gamma^{|q_2-q_1|},$$

where $\gamma = \alpha_1'\alpha_2''$ or $\alpha_1''\alpha_2'$, we have for all $q_1, q_2 \leqslant q$, $r < r_0$, $s < s_0$

$$\left|\overline{(n_1q_1 + n_2q_2)^s (\alpha_1'\alpha_2')^{pqr} \alpha_1^{pq_1r} \alpha_2^{pq_2r}}\right| \leqslant \exp(s_0 \log 2Hq + bpqr_0).$$

Setting in Lemma 3 $P = r_0 s_0$, $Q = (q+1)^2$ and taking into account that $r_0 s_0 \leqslant \frac{1}{3}q^2$ we infer that there exist integers $B_{q_1q_2}$ of R such that

$$L_{rs}([B_{q_1q_2}]) = 0, \qquad 0 \leqslant r < r_0,\ 0 \leqslant s < s_0 \tag{26}$$

and

$$0 < \max_{q_1,q_2}\left|\overline{B_{q_1q_2}}\right| < C^{3/2}(q+1)\exp(\tfrac{1}{2}\,s_0 \log 2Hq + \tfrac{1}{2}\,bpqr_0). \tag{27}$$

Setting

$$Q(r,s) = \sum_{q_1=0}^{q}\sum_{q_2=0}^{q} B_{q_1q_2}(n_1q_1 + n_2q_2)^s \alpha_1^{pq_1r}\alpha_2^{pq_2r} \qquad (r, s \text{ integers} \geqslant 0)$$

we have by (26)

$$Q(r,s) = 0 \quad \text{for} \quad 0 \leqslant r < r_0,\ 0 \leqslant s < s_0.$$

It is impossible that

$$Q(r, s) = 0 \quad \text{for} \quad 0 \leqslant r < (q+1)^2,\ 0 \leqslant s < s_0,$$

since already the system of $(q+1)^2$ linear equations for $B_{q_1q_2}$:

$$Q(r, 0) = 0 \quad (0 \leqslant r < (q+1)^2)$$

has the determinant

$$\det[a_1^{pq_1r}a_2^{pq_2r}] = \prod_{\langle q_1', q_2'\rangle \neq \langle q_1, q_2\rangle} (a_1^{pq_1}a_2^{pq_2} - a_1^{pq_1'}a_2^{pq_2'}),$$

which does not vanish as a consequence of the irrationality of η_2/η_1.

Let r_1 be the least positive integer such that $Q(r_1, s_1) \neq 0$ for some $s_1 < s_0$. Clearly

$$Q(r, s) = 0 \quad \text{for} \quad 0 \leqslant r < r_1,\ 0 \leqslant s < s_0, \tag{28}$$

$$Q(r_1, s_1) \neq 0, \quad \text{where} \quad r_0 \leqslant r_1 < (q+1)^2,\ 0 \leqslant s_1 < s_0. \tag{29}$$

By (27) we find

$$\begin{aligned}\overline{|(a_1'a_2')^{pqr_1}Q(r_1, s_1)|} &< C^{3/2}(q+1)^3\exp(\tfrac{1}{2}s_0\log 2Hq + \tfrac{1}{2}bpqr_0)\times\\ &\times\max_{q_1,q_2}\overline{|(n_1q_1+n_2q_2)^{s_1}(a_1'a_2')^{pqr_1}a_1^{pq_1r_1}a_2^{pq_2r_1}|}\\ &\leqslant C^{3/2}(q+1)^3\exp\left(\tfrac{3}{2}s_0\log 2Hq + bpq\frac{r_0+2r_1}{2}\right).\end{aligned}$$

This inequality together with (29) gives by Lemma 1

$$\begin{aligned}&\operatorname{ord}_p(a_1'a_2')^{pqr_1}Q(r_1, s_1)\\ &\quad< \mu\left(\frac{3}{2}\log C(q+1)^2 + \frac{3}{2}s_0\log 2Hq + bpq\frac{r_0+2r_1}{2}\right).\end{aligned} \tag{30}$$

Put now

$$\omega_0 = \operatorname{ord}_p\left(\frac{\eta_2}{\eta_1} - \frac{n_2}{n_1}\right),$$

$$f_0(z) = \sum_{q_1=0}^{q}\sum_{q_2=0}^{q} B_{q_1q_2}e(q_1\eta_1z + q_2\eta_2z).$$

By Lemma 5, $f_0(z)$ is a normal function on R_p and for all integers $r, s \geqslant 0$

$$f_0^{(s)}(pr) = \sum_{q_1=0}^{q}\sum_{q_2=0}^{q} B_{q_1q_2}(q_1\eta_1 + q_2\eta_2)^s a_1^{pq_1r}a_2^{pq_2r}.$$

Hence

$$\begin{aligned}&\operatorname{ord}_p\left(\eta_1^{-s}f_0^{(s)}(pr) - n_1^{-s}Q(r, s)\right)\\ &\quad= \operatorname{ord}_p\sum_{q_1=0}^{q}\sum_{q_2=0}^{q} B_{q_1q_2}\left(\left(q_1 + \frac{\eta_2}{\eta_1}q_2\right)^s - \left(q_1 + \frac{n_2}{n_1}q_2\right)^s\right)a_1^{pq_1r}a_2^{pq_2r}.\end{aligned}$$

If $\operatorname{ord}_p n_2/n_1 < 0$, we have $\omega_0 < 0$, whence the assertion of the lemma follows. If $\operatorname{ord}_p n_2/n_1 \geqslant 0$ we get for all $r, s \geqslant 0$

$$\operatorname{ord}_p\left(f_0^{(s)}(pr) - \frac{\eta_1^s}{n_1^s}Q(r, s)\right) \geqslant \omega_0. \tag{31}$$

It follows by (28) that $\operatorname{ord}_p f^{(s)}(pr) \geqslant \omega_0$ $(0 \leqslant r < r_1, 0 \leqslant s < s_0)$ and by Lemma 4

$$\operatorname{ord}_p f^{(s_1)}(pr_1) \geqslant \min\left\{\varphi(r_1s_0 - s_1),\ -\varphi(s_0+s_1)\frac{\log pr_1}{\log p} + \omega_0\right\}.$$

Applying (31) for $r = r_1, s = s_1$, we get

$$\operatorname{ord}_p\frac{\eta_1^{s_1}}{n_1^{s_1}}Q(r_1, s_1) \geqslant \min\left\{\varphi(r_1s_0 - s_1),\ -\varphi(s_0+s_1)\frac{\log pr_1}{\log p} + \omega_0\right\}$$

and since $s_1 < s_0$, $\operatorname{ord}_p n_1 \geqslant 0$, $\operatorname{ord}_p a_1'a_2' \geqslant 0$

$$\begin{aligned}&\operatorname{ord}_p(a_1'a_2')^{pqr_1}Q(r_1, s_1)\\ &\qquad\geqslant -s_0\operatorname{ord}_p\eta_1 + \min\left\{\varphi s_0(r_1-1),\ -2\varphi s_0\frac{\log pr_1}{\log p} + \omega_0\right\}.\end{aligned}$$

The comparison of this inequality with (30) gives

$$\begin{aligned}&-s_0\operatorname{ord}_p\eta_1 + \min\left\{\varphi s_0(r_1-1),\ -2\varphi s_0\frac{\log pr_1}{\log p} + \omega_0\right\}\\ &\qquad\leqslant \mu\left(\frac{3}{2}\log C(q+1)^2 + \frac{3}{2}s_0\log 2Hq + bpq\frac{r_0+2r_1}{2}\right).\end{aligned}$$

It follows that at least one of the following inequalities holds

$$(\varphi s_0 - \mu bpq)r_1 - \varphi s_0 - E \leqslant 0 \tag{32}$$

or

$$-\mu bpqr_1 - 2\varphi s_0\frac{\log pr_1}{\log p} + \omega_0 - E \leqslant 0, \tag{33}$$

where

$$E = s_0\operatorname{ord}_p\eta_1 + \tfrac{1}{2}\mu(3\log C(q+1)^2 + 3s_0\log 2Hq + bpqr_0).$$

We prove that (32) is impossible by showing that

$$\varphi s_0 - \mu bpq > 0, \tag{34}$$

$$(\varphi s_0 - \mu bpq) r_0 - \varphi s_0 - E > 0. \tag{35}$$

(34) follows directly from the definition of s_0. To show (35) we estimate its left hand side as follows

$$\begin{aligned}
&(\varphi s_0 - \mu bpq) r_0 - \varphi s_0 - E \\
&\quad = (\varphi s_0 - \tfrac{3}{2}\mu bpq) r_0 - (\operatorname{ord}_{\mathfrak{p}} \eta_1 + \tfrac{3}{2}\log 2Hq + \varphi) s_0 - \tfrac{3}{2}\mu \log C(q+1)^2 \\
&\quad > \left(\frac{3}{2}\mu bpq - \varphi\right)\left(\frac{\varphi q}{9\mu bp} - 1\right) - \\
&\qquad - (\operatorname{ord}_{\mathfrak{p}} \eta_1 + \tfrac{3}{2}\mu \log 2Hq + \varphi) 3\mu\varphi^{-1} bpq - \tfrac{3}{2}\mu \log C - 3\mu q \\
&\quad = \frac{\varphi}{6}\left(q^2 - 27\mu^2\varphi^{-2} bpq \log 2Hq - 18\mu\varphi^{-3} bpq \operatorname{ord}_{\mathfrak{p}} \eta_1 - \right. \\
&\qquad \left. - 27\mu\varphi^{-1} bpq - \frac{2\varphi}{3\mu bp} q - 18\mu\varphi^{-1} q - 9\mu\varphi^{-1} \log C + 6\right).
\end{aligned}$$

Since $\mu\varphi^{-1} bp \geqslant 1$, (35) follows now from (25). Therefore, (32) is excluded and (33) holds. Since $r_1 \leqslant (q+1)^2 - 1$ we get by (35)

$$\begin{aligned}
\omega_0 &\leqslant \mu bpq(q^2+2q) + 6\mu bpq \frac{\log p r_1}{\log p} + E \\
&< \mu bpq(q^2+2q-r_0) + \varphi s_0 \left(r_0 - 1 + 2\frac{\log p r_1}{\log p}\right) \\
&< \mu bpq\left(q^2+2q+2r_0+3+12\frac{\log(q+1)}{\log p}\right) \leqslant \mu bp(q+1)^3.
\end{aligned}$$

Proof of Theorem 1. Since the theorem is invariant with respect to the substitutions $\alpha = 1/\overline{\alpha}$, $n = -\overline{n}$; $\beta = 1/\overline{\beta}$, $m = -\overline{m}$ we can assume that $n \geqslant 0$, $m \geqslant 0$. The number

$$F = (\alpha'\beta')^N(\alpha^n - \beta^m) \neq 0$$

is an integer of R. Further

$$\overline{|F|} \leqslant \max\{|\overline{\alpha'\beta'}|, |\overline{\alpha''\beta''}|\}^N + \max\{|\overline{\alpha'\beta'}|, |\overline{\alpha'\beta''}|\}^N < 2\exp aN$$

and by Lemma 1

$$\operatorname{ord}_{\mathfrak{p}}(\alpha^n - \beta^m) \leqslant \operatorname{ord}_{\mathfrak{p}} F \leqslant \mu \log \overline{|F|} < \mu aN + \mu \log 2.$$

Thus the theorem certainly holds if

$$\mu aN + \mu \log 2 \leqslant 10^6 \mu^7 \varphi^{-2} a^4 p^{4\varrho+4}(\log N + \varphi a p^\varrho + 2a^{-1})$$

and we can assume that

$$N > 10^6 \mu^6 \varphi^{-2} a^3 p^{4\varrho+4}(\log N + \varphi a p^\varrho + 2a^{-1})^3 - a^{-1}\log 2.$$

Now by Minkowski's estimation for $|D|$

$$\nu a \geqslant \frac{1}{\nu}\log|eD| \geqslant 1, \qquad \mu a \geqslant \frac{1}{\varrho \log p}. \tag{36}$$

On the other hand,

$$\frac{p^{7\varrho+4}}{(\varrho\log p)^6} \geqslant \frac{2^{11}}{(\log 2)^6} \geqslant \exp 9.$$

Hence

$$N > 10^6(\nu a)^6 \frac{p^{7\varrho+4}}{(\varrho\log p)^6} > \exp 23,$$

$$N > 10^6 \frac{p^{4\varrho+4}}{(\varrho\log p)^6}\left(\frac{\nu}{\varphi}\log N + p^\varrho\right)^3 > 10^6 \frac{2^8}{(\log 2)^6}\cdot 25^3 > \exp 30,$$

$$\frac{\log N + \varphi a p^\varrho + 2a^{-1}}{\log(\log N + \varphi a p^\varrho + 2a^{-1})} > 9. \tag{37}$$

If α^n/β^m is a root of unity, the theorem follows at once since then by Lemma 1

$$\operatorname{ord}_{\mathfrak{p}}(\alpha^n - \beta^m) = \operatorname{ord}_{\mathfrak{p}}(\alpha^n/\beta^m - 1) \leqslant \mu \log 2.$$

The same inequality holds if only one of α, β is a $\mathfrak{p}$-adic unit.

If α^n/β^m is not a root of unity and α, β are both $\mathfrak{p}$-adic units, let σ be the least non-negative integer such that

$$p^\sigma \min\{\operatorname{ord}_{\mathfrak{p}}(\alpha^{p^\varrho-1} - 1), \operatorname{ord}_{\mathfrak{p}}(\beta^{p^\varrho-1} - 1)\} > \frac{\varphi}{p-1}.$$

(Such integers exist, since in virtue of Fermat theorem

$$\varkappa = \operatorname{ord}_{\mathfrak{p}}(\alpha^{p^\varrho-1} - 1) > 0 \quad \text{and} \quad \operatorname{ord}_{\mathfrak{p}}(\beta^{p^\varrho-1} - 1) > 0.)$$

We may assume without loss of generality that

$$\operatorname{ord}_{\mathfrak{p}}(\beta^{p^\sigma(p^\varrho-1)} - 1) \geqslant \operatorname{ord}_{\mathfrak{p}}(\alpha^{p^\sigma(p^\varrho-1)} - 1) \tag{38}$$

and set

$$\alpha_1 = \alpha^{p^\sigma(p^\varrho-1)}, \qquad \alpha_2 = \beta^{p^\sigma(p^\varrho-1)}. \tag{39}$$

We have

$$\frac{\alpha_1 - 1}{\alpha^{p^\varrho-1} - 1} \equiv (\alpha^{p^\varrho-1} - 1)^{p^\sigma-1} \bmod p,$$

thus by the choice of σ and (38)

$$\text{ord}_{\mathfrak{p}}(\alpha_2-1) \geqslant \text{ord}_{\mathfrak{p}}(\alpha_1-1) \geqslant \min\{p^{\sigma}\varkappa, \varphi+\varkappa) > \frac{\varphi}{p-1}. \tag{40}$$

Let η_i be the $\mathfrak{p}$-adic logarithm of α_i, η the $\mathfrak{p}$-adic logarithm of $\alpha_1^n\alpha_2^{-m}$. Since α^n/β^m is not a root of unity we have $\eta \neq 0$ and by (40) $\eta_1 \neq 0$, hence by Lemma 5

$$\begin{aligned}\text{ord}_{\mathfrak{p}}(\alpha^n-\beta^m) &\leqslant \text{ord}_{\mathfrak{p}}(\alpha_1^n-\alpha_2^m) = \text{ord}_{\mathfrak{p}}(\alpha_1^n\alpha_2^{-m}-1) \\ &= \text{ord}_{\mathfrak{p}}\eta = \text{ord}_{\mathfrak{p}}(n\eta_1-m\eta_2) = \text{ord}_{\mathfrak{p}}\eta_1+\text{ord}_{\mathfrak{p}}\left(n-m\frac{\eta_2}{\eta_1}\right).\end{aligned} \tag{41}$$

In order to estimate $\text{ord}_{\mathfrak{p}}\eta_1$ we notice that

$$\alpha_1 = \frac{\alpha_1''}{\alpha_1'}, \qquad \alpha_2 = \frac{\alpha_2''}{\alpha_2'}, \tag{42}$$

where

$$\begin{aligned}\alpha_1' &= \alpha'^{p^{\sigma}(p^{\varrho}-1)}, \qquad \alpha_1'' = \alpha''^{p^{\sigma}(p^{\varrho}-1)}, \\ \alpha_2' &= \beta'^{p^{\sigma}(p^{\varrho}-1)}, \qquad \alpha_2'' = \beta''^{p^{\sigma}(p^{\varrho}-1)}\end{aligned} \tag{43}$$

are integers of R. We have

$$b = \log\max\{|eD|^{1/p^2}, |\overline{\alpha_1'\alpha_2'}|, |\overline{\alpha_1'\alpha_2''}|, |\overline{\alpha_1''\alpha_2'}|, |\overline{\alpha_1''\alpha_2''}|\} \leqslant p^{\sigma}(p^{\varrho}-1)a$$

and since by the choice of σ

$$p^{\sigma} \leqslant p\frac{\varphi}{p-1} \leqslant 2\varphi,$$

it follows that

$$b \leqslant 2\varphi(p^{\varrho}-1)a. \tag{44}$$

If $\alpha_2 = 1$ we have by Lemma 5, Lemma 1, (42) and (43)

$$\begin{aligned}\text{ord}_{\mathfrak{p}}\eta_1 = \text{ord}_{\mathfrak{p}}(\alpha_1-1) &\leqslant \text{ord}_{\mathfrak{p}}(\alpha_1''-\alpha_1')\alpha_2' \\ &\leqslant \mu\log|\overline{(\alpha_1''-\alpha_1')\alpha_2'}| \leqslant \mu\log 2+\mu b.\end{aligned} \tag{45}$$

If $\alpha_2 \neq 1$ we have similarly

$$\begin{aligned}\text{ord}_{\mathfrak{p}}\eta_1 &\leqslant \tfrac{1}{2}\text{ord}_{\mathfrak{p}}\eta_1\eta_2 = \tfrac{1}{2}\text{ord}_{\mathfrak{p}}(\alpha_1-1)(\alpha_2-1) \\ &\leqslant \tfrac{1}{2}\text{ord}_{\mathfrak{p}}(\alpha_1''-\alpha_1')(\alpha_2''-\alpha_2') \leqslant \tfrac{1}{2}\mu\log|\overline{(\alpha_1''-\alpha_1')(\alpha_1''-\alpha_2')}| \\ &\leqslant \mu\log 2+\tfrac{1}{2}\mu b.\end{aligned} \tag{46}$$

It follows from (44), (45) and (46) that

$$\text{ord}_{\mathfrak{p}}\eta_1 \leqslant \begin{cases}\mu\log 2+2\mu\varphi(p^{\varrho}-1)a & \text{if} \quad \alpha_2 = 1, \\ \mu\log 2+\mu\varphi(p^{\varrho}-1)a & \text{if} \quad \alpha_2 \neq 1.\end{cases} \tag{47}$$

In order to estimate $\text{ord}_{\mathfrak{p}}\left(n-m\frac{\eta_2}{\eta_1}\right)$ and to complete the proof we distinguish two cases:

I. $m\eta_2/\eta_1$ is rational,

II. $m\eta_2/\eta_1$ is irrational.

I. If $m\eta_2 = 0$ we have

$$\text{ord}_{\mathfrak{p}}(n-m\eta_2/\eta_1) = \text{ord}_{\mathfrak{p}}n \leqslant \mu\log N. \tag{48}$$

If $m\eta_2 \neq 0$, let $\eta_2/\eta_1 = u_2/u_1$, where u_1, u_2 are rational integers and $(u_1, u_2) = 1$. By Lemma 5 we have

$$\alpha_1^{u_2} = e(u_2\eta_1) = e(u_1\eta_2) = \alpha_2^{u_1},$$

hence by (39)

$$\alpha^{p^{\sigma}(p^{\varrho}-1)u_2} = \beta^{p^{\sigma}(p^{\varrho}-1)u_1}. \tag{49}$$

α and β are not both roots of unity, therefore, we can apply to (49) Lemma 2 and we get

$$|u_1|+|u_2| \leqslant \nu a(2^{\nu+4}+1).$$

Hence by Lemma 1

$$\begin{aligned}\text{ord}_{\mathfrak{p}}(n-m\eta_2/\eta_1) = \text{ord}_{\mathfrak{p}}(n-mu_2/u_1) &\leqslant \text{ord}_{\mathfrak{p}}(nu_1-mu_2) \\ &\leqslant \mu\log|\overline{nu_1-mu_2}| \leqslant \mu\log N+\mu\log\nu a(2^{\nu+4}+1) \\ &\leqslant \mu\log N+\mu\log\nu a+\mu(\nu+3).\end{aligned} \tag{50}$$

It follows from (41), (47), (48) and (50) that in the present case

$$\text{ord}_{\mathfrak{p}}(\alpha^n-\beta^m) \leqslant \mu\log 2+2\mu\varphi(p^{\varrho}-1)a+\mu\log N+\mu\log\nu a+\mu(\nu+3).$$

This implies the theorem in view of (36).

II. Since $m \neq 0$ we have

$$\text{ord}_{\mathfrak{p}}\left(n-m\frac{\eta_2}{\eta_1}\right) = \text{ord}_{\mathfrak{p}}\left(\frac{\eta_2}{\eta_1}-\frac{n}{m}\right)+\text{ord}_{\mathfrak{p}}m. \tag{51}$$

α_1 and α_2 satisfy the assumptions of Lemma 6 and we can apply that lemma with $n_1 = m$, $n_2 = n$, $H = N$. We set

$$q = [78\mu^2\varphi^{-1}ap^{\varrho+1}(\log N+\varphi ap^{\varrho}+2a^{-1})]+1 > 156\mu^2\varphi^{-1}p^{\varrho+1}. \tag{52}$$

To show that q satisfies inequality (25) we proceed as follows. By (47) we have

$$\mu\log 2+\tfrac{2}{3}\operatorname{ord}_{\mathfrak{p}}\eta_1+\tfrac{83}{81}\varphi+\tfrac{2}{3}\mu<\tfrac{5}{3}\mu\log 2+\tfrac{2}{3}\mu\varphi(p^{\varrho}-1)a+\tfrac{83}{81}\varphi+\tfrac{2}{3}\mu$$
$$\leqslant\mu(\varphi ap^{\varrho}+2a^{-1}).$$

Hence by (44)

$$q-27\mu\varphi^{-2}bp(\mu\log 2N+\tfrac{2}{3}\operatorname{ord}_{\mathfrak{p}}\eta_1+\tfrac{83}{81}\varphi+\tfrac{2}{3}\mu)$$
$$\geqslant q-54\mu^2\varphi^{-1}ap^{\varrho+1}(\log N+\varphi ap^{\varrho}+2a^{-1})-54\mu^2\varphi^{-1}ap^{\varrho+1}\log q. \tag{53}$$

Since $x-t\log x$ is an increasing function for $x>t$ and $q>54\mu^2\varphi^{-1}ap^{\varrho+1}$ we have by (37)

$$\begin{aligned}&\frac{q}{\mu^2\varphi^{-1}ap^{\varrho+1}}-54(\log N+\varphi ap^{\varrho}+2a^{-1})-54\log q\\ &>78(\log N+\varphi ap^{\varrho}+2a^{-1})-54(\log N+\varphi ap^{\varrho}+2a^{-1})-\\ &\quad-54\log 78\mu^2\varphi^{-1}ap^{\varrho+1}-54\log(\log N+\varphi ap^{\varrho}+2a^{-1})\\ &>24(\log N+\varphi ap^{\varrho}+2a^{-1})-54\log 78\mu^2\varphi^{-1}ap^{\varrho+1}-\\ &\quad-\tfrac{54}{9}(\log N+\varphi ap^{\varrho}+2a^{-1})\\ &>18\log N+36a^{-1}-54\log 78\mu^2\varphi^{-1}ap^{\varrho+1}\\ &>18\log\frac{N}{(78\mu^2\varphi^{-1}ap^{\varrho+1})^3}+36a^{-1}>18a^{-1}(a+2).\end{aligned} \tag{54}$$

On the other hand, by Lemma 3

$$\log C<\tfrac{5}{2}\nu\log\nu+\tfrac{1}{2}\log|D|\leqslant\tfrac{5}{2}\nu\log\nu+\tfrac{1}{2}\nu^2a\leqslant\tfrac{1}{2}\nu^2(a+2). \tag{55}$$

It follows from (51), (52), (53) and (54) that

$$\begin{aligned}&q^2-27\mu\varphi^{-2}bpq(\mu\log 2Nq+\tfrac{2}{3}\operatorname{ord}_{\mathfrak{p}}\eta_1+\tfrac{83}{81}\varphi+\tfrac{2}{3}\mu)-9\mu\varphi^{-1}\log C\\ &>156\mu^2\varphi^{-1}p^{\varrho+1}\cdot 18\mu^2\varphi^{-1}p^{\varrho+1}(a+2)-9\mu\varphi^{-1}\cdot\tfrac{1}{2}\nu^2(a+2)\\ &=\tfrac{9}{2}\mu\varphi^{-1}(a+2)(624\mu^3\varphi^{-1}p^{2\varrho+2}-\nu^2)\\ &=\tfrac{9}{2}\mu\varphi^{-1}(a+2)\nu^2\left(624\nu\varphi^{-1}\frac{p^{2\varrho+2}}{(\varrho\log p)^3}-1\right)>0.\end{aligned}$$

Since the inequality (25) is satisfied we infer by Lemma 6 and (44) that

$$\operatorname{ord}_{\mathfrak{p}}\left(\frac{\eta_2}{\eta_1}-\frac{n}{m}\right)\leqslant\mu bp(q+1)^3\leqslant 2\mu\varphi ap^{\varrho+1}(q+1)^3. \tag{56}$$

However clearly

$$q+1\leqslant 79\mu^2\varphi^{-1}ap^{\varrho+1}(\log N+\varphi ap^{\varrho}+2a^{-1}) \tag{57}$$

and it follows from (41), (47), (51), (56) and (57) that

$$\begin{aligned}&\operatorname{ord}_{\mathfrak{p}}(\alpha^n-\beta^m)\\ &\leqslant\mu\log 2+\mu\varphi p^{\varrho}a+\log N+2\cdot 79^3\mu^7\varphi^{-2}a^4p^{4\varrho+4}(\log N+\varphi ap^{\varrho}+2a^{-1})^3\\ &<10^6\mu^7\varphi^{-2}a^4p^{4\varrho+4}(\log N+\varphi ap^{\varrho}+2a^{-1})^3\end{aligned}$$

which completes the proof.

LEMMA 7. *If $f(z)$ is an integral function satisfying the inequality*

$$|f(z)|<\exp(\lambda_0|z|+\lambda_1),$$

r_1, s_0, s_1 are integers, $r_1\geqslant 70$, $s_0\geqslant 3\lambda_0>0$, $s_1\geqslant 0$, and

$$M=\max_{\substack{0\leqslant r<r_1\\ 0\leqslant s<s_0}}|f^{(s)}(r)|,$$

then

$$|f^{(s_1)}(r_1)|\leqslant e^{r_1s_0+s_1\log s_1}\left(\frac{e^{\lambda_1}}{\lambda_0}\left(\frac{\lambda_0}{s_0}\right)^{r_1s_0}r_1^{2s_0}+M\right).$$

Proof. We have in virtue of Lagrange's interpolation formula

$$f(z)=\frac{1}{2\pi i}\int_{\Gamma_0}\frac{f(\xi)}{\xi-z}\left(\frac{z(z-1)\dots(z-r_1+1)}{\xi(\xi-1)\dots(\xi-r_1+1)}\right)^{s_0}d\xi-$$
$$-\sum_{r=0}^{r_1-1}\sum_{s=0}^{s_0-1}\frac{f^{(s)}(r)}{s!\,2\pi i}\int_{\Gamma_{r+1}}\frac{(\xi-r)^s}{\xi-z}\left(\frac{z(z-1)\dots(z-r_1+1)}{\xi(\xi-1)\dots(\xi-r_1+1)}\right)^{s_0}d\xi,$$

where Γ_0 is the circle $|\xi|=r_1s_0/\lambda_0$, Γ_{r+1} is the circle $|\xi-r|=\frac{1}{3}$, provided z lies inside Γ_0 but outside Γ_{r+1} $(0\leqslant r<r_1)$.

Let Δ be the circle $|z-r_1|=\frac{1}{2}$. If $z\in\Delta$ we have

$$|\xi-z|>|\xi|-r_1-\frac{1}{2}\geqslant\frac{r_1s_0}{\lambda_0}-\frac{3}{2}r_1>\frac{3}{2}r_1\quad(\xi\in\Gamma_0),$$
$$|\xi-z|>r_1-\tfrac{1}{2}-|\xi|\geqslant r_1-r-\frac{5}{6}\quad(\xi\in\Gamma_{r+1},\ r<r_1).$$

Hence for $z\in\Delta$

$$|f(z)|<\frac{r_1s_0}{\lambda_0}e^{r_1s_0+\lambda_1}\frac{2}{3r_1}\left|\frac{\Gamma(r_1+\frac{3}{2})\Gamma(\frac{3}{2})^{-1}}{\Gamma\left(\frac{r_1s_0}{\lambda_0}+1\right)\Gamma\left(\frac{r_1s_0}{\lambda_0}+1-r_1\right)^{-1}}\right|^{s_0}+$$
$$+\sum_{r=0}^{r_1-1}\sum_{s=0}^{s_0-1}\frac{1}{r_1-r-\frac{5}{6}}\cdot\frac{M}{s!}\cdot\frac{1}{3^{s+1}}\left|\frac{\Gamma(r_1+\frac{4}{3})\Gamma(\frac{4}{3})^{-1}}{\Gamma(r+\frac{2}{3})\Gamma(-\frac{1}{3})^{-1}\Gamma(r_1-r-\frac{1}{3})\Gamma(\frac{1}{3})^{-1}}\right|^{s_0}.$$

Since

$$\left(\frac{a-1}{e}\right)^{a-b} < \frac{\Gamma(a)}{\Gamma(b)} < \left(\frac{a}{e}\right)^{a}\left(\frac{b}{e}\right)^{-b} \qquad (a > b \geqslant 1),$$

we have

$$\Gamma\left(r_1+\frac{4}{3}\right)\Gamma\left(\frac{4}{3}\right)^{-1} < \Gamma\left(r_1+\frac{3}{2}\right)\Gamma\left(\frac{3}{2}\right)^{-1} < \left(\frac{r_1+\frac{3}{2}}{e}\right)^{r_1+\frac{3}{2}}\left(\frac{3}{2e}\right)^{-\frac{3}{2}}$$

$$< e^{-r_1-\frac{3}{2}} r_1^{r_1+\frac{3}{2}} e^{\frac{3}{2r_1}\left(r_1+\frac{3}{2}\right)+0,9} < r_1^{r_1+\frac{3}{2}} e^{-r_1+1},$$

$$\Gamma\left(\frac{r_1 s_0}{\lambda_0}+1\right)\Gamma\left(\frac{r_1 s_0}{\lambda_0}+1-r_1\right)^{-1} \geqslant \left(\frac{r_1 s_0}{e\lambda_0}\right)^{r_1}$$

and

$$|\Gamma(r+\tfrac{2}{3})\Gamma(r_1-r-\tfrac{1}{3})\Gamma(-\tfrac{1}{3})^{-1}\Gamma(\tfrac{2}{3})^{-1}|$$

$$\geqslant \left(\frac{r-\frac{1}{3}}{e}\right)^{r-1}\left(\frac{r_1-r-\frac{4}{3}}{e}\right)^{r_1-r-2}\Gamma(\tfrac{5}{3})^2|\Gamma(-\tfrac{1}{3})|^{-1}\Gamma(\tfrac{3}{2})^{-1}$$

$$\geqslant \tfrac{4}{21}e^{-r_1+3}(r-\tfrac{1}{3})^{r-1}(r_1-r-\tfrac{4}{3})^{r_1-r-2} \qquad (1 \leqslant r \leqslant r_1-2).$$

The differentiation shows that the last function takes its minimum for $r = (r_1-1)/2$. Thus

$$|\Gamma(r+\tfrac{3}{3})\Gamma(r_1-r-\tfrac{1}{3})\Gamma(-\tfrac{1}{3})^{-1}\Gamma(\tfrac{2}{3})^{-1}|$$

$$\geqslant \frac{4}{27}e^{-r_1+3}\left(\frac{r_1}{2}-\frac{5}{6}\right)^{r_1-3} \geqslant \frac{4}{27}e^{-r_1+3}\left(\frac{r_1}{2}\right)^{r_1-3} e^{-5(r_1-3)/(3r_1-5)}$$

$$\geqslant \frac{4}{27}e^{-r_1+3}\left(\frac{r_1}{2}\right)^{r_1-3} e^{-5/3} > r_1^{r_1-3}e^{-r_1+1}2^{-r_1}.$$

The same is true for $r = 0$ or r_1-1. Hence for $z \in \Delta$ we get

$$|f(z)| < \frac{2s_0}{3\lambda_0}e^{r_1 s_0+\lambda_1}\left(\frac{\lambda_0}{s_0}\right)^{r_1 s_0} r_1^{\frac{3}{2}s_0} e^{s_0} + (7+\log r_1)\frac{1}{3}e^{1/3}M(2^{r_1}r_1^{9/2})^{s_0}.$$

However, for $r_1 \geqslant 70$ and $s_0 \geqslant 1$

$$\tfrac{2}{3}s_0 r_1^{\frac{3}{2}s_0}e^{s_0} \leqslant \tfrac{1}{2}r_1^{2s_0}, \quad \tfrac{1}{3}e^{1/3}(7+\log r_1)(2^{r_1}r_1^{9/2})^{s_0} \leqslant \tfrac{1}{2}e^{r_1 s_0},$$

thus

$$|f(z)| < \frac{1}{2}e^{r_1 s_0}\left(\frac{e^{\lambda_1}}{\lambda_0}\left(\frac{\lambda_0}{s_0}\right)^{r_1 s_0} r_1^{2s_0}+M\right) \qquad (z \in \Delta).$$

Now, by Cauchy's theorem

$$f^{(s_1)}(r_1) = \frac{s_1!}{2\pi i}\int_{\Delta}\frac{f(z)}{(z-r_1)^{s_1+1}}\,dz,$$

and on the other hand $2^{s_1-1}s_1! \leqslant s_1^{s_1}$, thus

$$|f^{(s_1)}(r_1)| \leqslant 2^{s_1}s_1!\max_{z\in\Delta}|f(z)| \leqslant e^{r_1 s_0+s_1\log s_1}\left(\frac{e^{\lambda_1}}{\lambda_0}\left(\frac{\lambda_0}{s_0}\right)^{r_1 s_0} r_1^{2s_0}+M\right), \quad \text{q.e.d.}$$

LEMMA 8. *Let $\alpha_1, \alpha_2 \in R$, $\alpha_i = \alpha_i''/\alpha_i'$, where α_i', α_i'' are integers of R, $\alpha_1\alpha_2 \neq 0$, η_i be any complex logarithm of α_i such that $0 < |\eta_1| \geqslant |\eta_2|$ and*

$$c = \max\left\{\frac{1}{\nu}, \frac{|\eta_1|}{\nu}, \frac{|\eta_1+\eta_2|}{\nu}, \log\max\{|\overline{\alpha_1'\alpha_2'}|, |\overline{\alpha_1'\alpha_2''}|, |\overline{\alpha_1''\alpha_2'}|, |\overline{\alpha_1''\alpha_2''}|\}\right\}.$$

Suppose that $\eta_1 = 2\pi i$, η_2/η_1 is irrational or $\eta_1, \eta_2, 2\pi i$ are rationally independent. If $H > |\eta_1|$ and a positive integer q satisfies the inequalities

$$q > 1680\nu c, \tag{58}$$

$$q^2 - 40{,}4\nu cq(\nu\log 2Hq - \tfrac{2}{3}\log\eta_1 + \tfrac{4}{3}\log q + \tfrac{1}{4}\nu) - 6\log C > 0, \tag{59}$$

where C is the constant of Lemma 3, then

$$\log\left|\frac{\eta_2}{\eta_1}-\frac{n_2}{n_1}\right| > \begin{cases} -10\nu cq^2 & \text{if } \eta_1 = 2\pi i, \\ -9\nu c(q+1)^3 & \text{otherwise.}\end{cases} \tag{60}$$

Proof. We set

$$r_0 = \left[\frac{q}{24\nu c}\right], \qquad s_0 = [8\nu cq]$$

and since $0 < r_0 s_0 \leqslant \frac{1}{3}q^2$ we find, like in the proof of Lemma 6, integers $C_{q_1q_2}$ of R $(0 \leqslant q_1 \leqslant q, 0 \leqslant q_2 \leqslant q)$ such that

$$0 < \max_{q_1,q_2}|\overline{C_{q_1q_2}}| < C^{3/2}(q+1)\exp(\tfrac{1}{2}s_0\log 2Hq + \tfrac{1}{2}cqr_0) \tag{61}$$

and

$$P(r,s) = 0 \quad \text{for} \quad 0 \leqslant r < r_0,\ 0 \leqslant s < s_0,$$

where for all $r, s \geqslant 0$

$$P(r,s) = \sum_{q_1=0}^{q}\sum_{q_2=0}^{q} C_{q_1q_2}(n_1q_1+n_2q_2)^s \alpha_1^{q_1 r}\alpha_2^{q_2 r}.$$

Consider first the case $\eta_1 = 2\pi i$; $\alpha_1 = 1$. It is impossible that

$$P(r,s) = 0 \quad \text{for} \quad 0 \leqslant r \leqslant q,\ 0 \leqslant s < s_0,$$

since $q < s_0$ and already the system of $(q+1)^2$ linear equations for $C_{q_1q_2}$: $P(r,s) = 0$ for $0 \leqslant r \leqslant q, 0 \leqslant s \leqslant q$ has the determinant

$$\det[(n_1q_1+n_2q_2)^s a_2^{q_2r}] = \prod_{q_2 \neq q_2'} (a_2^{q_2} - a_2^{q_2'}) \prod_{q_2=0}^{q} \prod_{q_1 \neq q_1'} (n_1q_1 - n_1q_1'),$$

which does not vanish as the consequence of the irrationality of η_2/η_1.

Therefore, there exist integers r_1 and s_1 such that

$$P(r,s) = 0 \quad \text{for} \quad 0 \leqslant r < r_1,\ 0 \leqslant s < s_0, \tag{62}$$

$$P(r_1, s_1) \neq 0 \tag{63}$$

and

$$r_0 \leqslant r_1 \leqslant q, \quad 0 \leqslant s_1 < s_0. \tag{64}$$

If $\eta_1, \eta_2, 2\pi i$ are rationally independent we obtain again (62) and (63) but now we can conclude only that

$$r_0 \leqslant r < (q+1)^2, \quad 0 \leqslant s_1 < s_0, \tag{65}$$

since we use the fact that the system of equations $P(r,0) = 0$ $(0 \leqslant r < (q+1)^2)$ has a nonvanishing determinant. Put

$$\lambda_1 = \tfrac{3}{2}\log C(q+1)^2 + \tfrac{1}{2}s_0 \log 2Hq + \tfrac{1}{2}cqr_0. \tag{66}$$

By (61) we get

$$\overline{|(a_1'a_2')^{qr_1}P(r_1,s_1)|} \leqslant e^{\lambda_1} \max_{a_1,a_2} \overline{|(n_1q_1+n_2q_2)^{s_1}(a_1'a_2')^{qr_1}a_1^{q_1r_1}a_2^{q_2r_1}|}$$
$$\leqslant \exp(\lambda_1 + s_0\log 2Hq + cqr_1).$$

Hence by (63) and Lemma 1

$$\log|(a_1'a_2')^{qr_1}P(r_1,s_1)| > -(\nu-1)(\lambda_1 + s_0\log 2Hq + cqr_1). \tag{67}$$

Put now

$$\omega_1 = -\log\left|\frac{\eta_2}{\eta_1} - \frac{n_2}{n_1}\right|,$$

$$f_1(z) = \sum_{q_1=0}^{q}\sum_{q_2=0}^{q} C_{q_1q_2}\exp(q_1\eta_1 z + q_2\eta_2 z).$$

We have

$$|q_1\eta_1 z + q_2\eta_2 z| \leqslant q|z|\max\{|\eta_1|, |\eta_2|, |\eta_1+\eta_2|\} \leqslant vcq|z|.$$

Thus, the function $f_1(z)$ satisfies the assumptions of Lemma 7 with $\lambda_0 = vcq$.

By Lagrange's theorem we have for any $r, s \geqslant 0$ and for some

$$x_{rs} = n_2/n_1 + t_{rs}(\eta_2/\eta_1 - n_2/n_1) \quad (0 < t_{rs} < 1)$$

$$\eta_1^{-s}f_1^{(s)}(r) - n_1^{-s}P(r,s) = e^{-\omega_1}\frac{d}{dx}\left(\sum_{q_1=0}^{q}\sum_{q_2=0}^{q} C_{q_1q_2}(q_1+xq_2)^s a_1^{q_1r}a_2^{q_2r}\right)\Big|_{x=x_{rs}}$$
$$= e^{-\omega_1}\sum_{q_1=0}^{q}\sum_{q_2=0}^{q} C_{q_1q_2}sq_2(q_1+x_{rs}q_2)^{s-1}a_1^{q_1r}a_2^{q_2r}.$$

If $|x_{rs}| > 1$ we get

$$|n_2/n_1| > 1 \geqslant |\eta_2/\eta_1| \quad \text{and} \quad |\eta_2/\eta_1 - n_2/n_1| > 1/|n_1| \geqslant 1/H,$$

whence (60) follows in view of (58) and (59).

If $|x_{rs}| \leqslant 1$ we get by (61) and (66)

$$|f_1^{(s)}(r) - \frac{\eta_1^s}{n_1^s}P(r,s)| \leqslant \exp\big(vcs - \omega_1 + \lambda_1 + s\log eq + qr(c - \log|a_1'a_2'|)\big). \tag{68}$$

It follows from (62) and (68) that for all $r < r_1$ and $s < s_0$

$$|f_1^{(s)}(r)| \leqslant \exp\big(-\omega_1 + \lambda_1 + s_0(\log eq + vc) + qr_1(c - \log|a_1'a_2'|)\big).$$

The numbers r_1 and s_0 satisfy the assumptions of Lemma 7 since by (58) $r_1 \geqslant r_0 \geqslant 70$, $s_0 \geqslant 8vcq - 1 > 3vcq = 3\lambda_0$. Applying that lemma we obtain

$$|f_1^{(s_1)}(r_1)| \leqslant \exp(r_1s_0 + s_1\log s_1)\left(\frac{\exp\lambda_1}{vcq}\left(\frac{vcq}{s_0}\right)^{r_1s_0} r_1^{2s_0} + \right.$$
$$\left. + \exp\big(-\omega_1 + \lambda_1 + s_0(\log eq + vc) + qr_1(c - \log|a_1'a_2'|)\big)\right).$$

Applying now (68) for $r = r_1, s = s_1$ we get

$$\left|\frac{\eta_1^{s_1}}{n_1^{s_1}}P(r_1,s_1)\right| \tag{69}$$
$$\leqslant 3\exp\max\left\{r_1s_0 + s_1\log s_1 + \lambda_1 + r_1s_0\log\frac{vcq}{s_0} + 2s_0\log r_1,\right.$$
$$r_1s_0 + s_1\log s_1 + \omega_1 + \lambda_1 + s_0(\log eq + vc) + qr_1(c - \log|a_1'a_2'|),$$
$$\left. vcs_1 - \omega_1 + \lambda_1 + s_1\log eq + qr_1(c - \log|a_1'a_2'|)\right\}.$$

Since $s_1 < s_0$ and $H > |\eta_1|$ we have

$$s_1\log\left|\frac{n_1}{\eta_1}\right| \leqslant s_1\log\frac{H}{|\eta_1|} < s_0\log\frac{H}{|\eta_1|}. \tag{70}$$

It follows from (69) and (70) that

$$\log|(a_1'a_2')^{qr_1}P(r_1,s_1)|$$
$$<qr_1\log|a_1'a_2'|+s_0\log\frac{H}{|\eta_1|}+\log 3+r_1s_0+s_0\log s_0+\lambda_1+$$
$$+\max\left\{s_0\left(r_1\log\frac{\nu cq}{s_0}+2\log r_1\right),-\omega_1+qr_1(c-\log|a_1'a_2'|)+s_0(\log eq+\nu c)\right\}.$$

Since $\log|a_1'a_2'|<c$, the comparison of this inequality with (67) gives

$$cqr_1+s_0\log\frac{H}{|\eta_1|}+r_1s_0+s_0\log s_0+\lambda_1+$$
$$+\max\left\{s_0\left(r_1\log\frac{\nu cq}{s_0}+2\log r_1\right),-\omega_1+s_0(\log eq+\nu c)\right\}$$
$$>-(\nu-1)(\lambda_1+s_0\log 2Hq+cqr_1).$$

It follows that at least one of the following inequalities holds

$$r_1\left(\nu cq+s_0+s_0\log\frac{\nu cq}{s_0}+2s_0\frac{\log r_1}{r_1}\right)+G>0 \tag{71}$$

or

$$r_1(\nu cq+s_0)-\omega_1+s_0(\log eq+\nu c)+G>0, \tag{72}$$

where

$$G=\nu s_0\log 2Hq+\nu\lambda_1+s_0\log\frac{s_0}{2|\eta_1|q}+\log 3$$
$$=\frac{3}{2}\nu s_0\log 2Hq+\frac{3}{2}\nu\log C(q+1)^2+\frac{1}{2}\nu cqr_0+s_0\log\frac{s_0}{2|\eta_1|q}+\log 3.$$

We prove that (71) is impossible by showing that

$$\nu cq+s_0+s_0\log\frac{\nu cq}{s_0}+2s_0\frac{\log r_0}{r_0}<0,$$

$$r_0\left(\nu cq+s_0+s_0\log\frac{\nu cq}{s_0}+2s_0\frac{\log r_0}{r_0}\right)+G<0. \tag{73}$$

We notice first that

$$\nu cq+s_0+s_0\log\frac{\nu cq}{s_0}+2s_0\frac{\log r_0}{r_0}$$
$$<s_0\left(\frac{1}{8}+\frac{1}{8\nu cq-1}+1-\log\frac{8\nu cq-1}{\nu cq}+\frac{2}{e}\right)<s_0(2-\log 8)<0.$$

To show (73) we estimate its left hand side as follows

$$r_0\left(\nu cq+s_0+s_0\log\frac{\nu cq}{s_0}+2s_0\frac{\log r_0}{r_0}\right)+G$$
$$<r_0\left(\frac{3}{2}\nu cq+s_0-s_0\log 8+\frac{s_0}{8\nu cq-1}\right)+$$
$$+s_0\left(\frac{3}{2}\nu\log 2Hq+\log\frac{s_0r_0^2}{2|\eta_1|q}\right)+\frac{3}{2}\nu\log C(q+1)^2+\log 3$$
$$<\left(\frac{q}{24\nu c}-1\right)\left(\frac{3}{2}\nu cq-(8\nu cq-1)\left(\log 8-1-\frac{1}{8\nu cq-1}\right)\right)+$$
$$+8\nu cq\left(\frac{3}{2}\nu\log 2Hq+\log\frac{q^2}{144|\eta_1|\nu c}+\frac{3}{8}\nu\right)+\frac{3}{2}\nu\log C+\log 3$$
$$\leqslant-\frac{8\log 8-9{,}5}{24}q^2+\nu cq(12\nu\log 2Hq-8\log|\eta_1|+16\log q+3\nu)+\frac{3}{2}\nu\log C$$
$$=-\frac{8\log 8-9{,}5}{24}\left(q^2-40{,}4\nu cq\left(\nu\log 2Hq-\frac{2}{3}\log|\eta_1|+\frac{4}{3}\log q+\frac{1}{4}\nu\right)-6\nu\log C\right).$$

It follows now from (59) that (73) holds. Thus (72) must be true and we get from (64) or (65), respectively, if $\eta_1=2\pi i$

$$\omega_1\leqslant q(\nu cq+s_0)+s_0(\log eq+\nu c)-r_0\left(\nu cq+s_0+s_0\log\frac{\nu cq}{s_0}+2s_0\frac{\log r_0}{r_0}\right)$$
$$=\nu cq^2+s_0\left(q+\log eq+\nu c+r_0\left(\log\frac{s_0}{\nu cq}-\frac{9}{8}\right)\right)$$
$$=\nu cq^2+8\nu cq\left(q+\log eq+\nu c+\frac{q}{24\nu c}\left(\log 8-\frac{9}{8}\right)\right)\leqslant 10\nu cq^2,$$

otherwise

$$\omega_1\leqslant(q^2+2q)(\nu cq+s_0)+s_0(\log eq+\nu c)-r_0\left(\nu cq+s_0+s_0\log\frac{\nu cq}{s_0}+2s_0\frac{\log r_0}{r_0}\right)$$
$$=\nu cq^3+2\nu cq^2+s_0\left(q^2+2q+\log eq+\nu c+r_0\left(\log\frac{s_0}{\nu cq}-1-\frac{\nu cq}{s_0}\right)\right)$$
$$=\nu cq^3+2\nu cq^2+8\nu cq\left(q^2+2q+\log eq+\frac{q}{1680}+\frac{q}{24\nu c}\left(\log 8-\frac{9}{8}\right)\right)$$
$$<9\nu c(q+1)^3.$$

COROLLARY 1. *If γ is an algebraic integer $\neq 0$, $\gamma/|\gamma|$ is not a root of unity and $H>1$, then*

$$\left|\frac{1}{2\pi}\arg\gamma-\frac{n_1}{n_2}\right|>\exp\bigl(-c(\gamma)\log^2 H\bigr),$$

where $c(\gamma)$ is independent of n_1, n_2.

Proof. This follows from Lemma 8 on taking $a_1=1$, $\eta_1=2\pi i$, $a_2=\gamma/|\gamma|$, $\eta_2=i\arg\gamma$ and $q=c_1(\gamma)\log H$, where $c_1(\gamma)$ is a sufficiently large constant.

Proof of Theorem 2. We can assume like in the proof of Theorem 1 that $n\geqslant 0$, $m\geqslant 0$. If α^n/β^m is a root of unity the theorem follows at once since then by Lemma 1

$$\log|\alpha^n-\beta^m|-\max\{n\log|\alpha|, m\log|\beta|\}=\log|\alpha^n/\beta^m-1|\geqslant-(\nu-1)\log 2.$$

If α^n/β^m is not a root of unity, we consider separately three cases:

I. $|\alpha|=|\beta|=1$ and $\alpha^u=\beta^v$ for some integers u, v not both 0,

II. $|\alpha|\neq 1$ or $|\beta|\neq 1$ and $u_0\log|\alpha|-v_0\log|\beta|=0$, where $(u_0, v_0)=1$, $u_0\geqslant 0$,

III. $|\alpha|^u\neq|\beta|^v$ for all integers u, v not both 0.

I. Here $\nu\geqslant 2$. The number

$$I=(\alpha'\beta')^N(\alpha^n-\beta^m)\neq 0$$

is an integer of R, $|\overline{I}|<2\exp aN$ and by Lemma 1

$$\log|\alpha^n-\beta^m|\geqslant-\log|\alpha'\beta'|^N-(\nu-1)\log 2-(\nu-1)aN>-\nu aN-\nu\log 2.$$

Thus, the theorem certainly holds if

$$\nu aN+\nu\log 2\leqslant 10^5\nu^5 a_1^3(\log N+\nu)^2$$

and we can assume that

$$N>10^5\nu^4 a_1^2(\log N+\nu)^2-a^{-1}\log 2.$$

Since $\nu\geqslant 2$, $\nu a\geqslant 1$, $\nu a_1\geqslant 2\pi$, we have

$$N>10^5\nu^4(\nu a_1)^2-\nu>\exp 16,$$

$$\log(\log N+\nu)\leqslant 2+\frac{\log N+\nu}{15}, \tag{74}$$

$$N>10^4 e^4\nu^4 a_1^2. \tag{75}$$

We set in Lemma 8: $a_1=1$, $a_2=\alpha\beta^{\pm 1}$, where the sign is chosen so that $|v\pm u|=|u|+|v|$, $\alpha_1'=\alpha_1''=1$,

$$\langle\alpha_2', \alpha_2''\rangle=\begin{cases}\langle\alpha'\beta', \alpha''\beta''\rangle & \text{for the upper sign,}\\ \langle\alpha'\beta'', \alpha''\beta'\rangle & \text{for the lower sign,}\end{cases}$$

$\eta_1=2\pi i$, $\eta_2=i\arg a_2-2\pi i$. The quotient η_2/η_1 is irrational, since otherwise $\alpha\beta^{\pm 1}$ would be a root of unity, and since $(\alpha\beta^{\pm 1})^\nu=\alpha^{\nu\pm u}$, α, β and α^n/β^m would be such roots.

Since $|\eta_1+\eta_2|\leqslant|\eta_1|=2\pi$, we have

$$c\leqslant\max\left\{\frac{2\pi}{\nu}, a\right\}=a_1. \tag{76}$$

On the other hand, since $\alpha^u=\beta^v$ we have by Lemma 2

$$\frac{|u|+|v|}{(u, v)}\leqslant\nu a(2^{\nu+4}+1). \tag{77}$$

Let k be the least positive integer such that

$$\alpha^{\frac{u}{(u,v)}k}=\beta^{\frac{v}{(u,v)}k}.$$

Clearly k does not exceed the number w of roots of unity contained in R and since $\varphi(w)\leqslant\nu$ we have

$$k\leqslant w\leqslant 2\nu^2. \tag{78}$$

We set in Lemma 8

$$n_1=7k\frac{n\nu-mu}{(u, v)},\qquad n_2=7\left[\frac{n_1}{7}\cdot\frac{\eta_2}{\eta_1}+\frac{1}{2}\right],$$

$$q=[99\nu^2 a_1(\log N+\nu)]+1.$$

Since α^n/β^m is not a root of unity, we have $n\nu-mu\neq 0$, thus

$$H\geqslant|n_1|\geqslant 7>|\eta_1|.$$

On the other hand, since $|\eta_2|\leqslant|\eta_1|$ we have $|n_2|\leqslant|n_1|$ and by (76), (77) and (78)

$$H\leqslant 14\nu^3 a(2^{\nu+4}+1)N\leqslant e^{\nu}N^{3/2}.$$

It is clear that q satisfies (58). To show that q satisfies (59) we proceed as follows

$$\nu\log 2H-\tfrac{2}{3}\log|\eta_1|+\tfrac{1}{4}\nu\leqslant\nu\log 2+\nu^2+\tfrac{3}{2}\nu\log N-\tfrac{2}{3}\log 2\pi+\tfrac{1}{4}\nu\leqslant\tfrac{3}{2}\nu(\log N+\nu).$$

Hence by (76)

$$(79)\quad q-40{,}4\nu c(\nu\log 2Hq-\tfrac{2}{3}\log|\eta_1|+\tfrac{4}{3}\log q+\tfrac{1}{4}\nu)$$
$$\geqslant q-60{,}6\nu^2a_1(\log N+\nu)-67{,}4\nu^2a_1\log q.$$

Since $x-t\log x$ is an increasing function for $x>t$ and

$$(80)\qquad q>99\nu^2a_1(\log N+\nu)>67{,}4\nu^2a_1$$

we have by (74) and (75)

$$(81)\quad \frac{q}{\nu^2a_1}-60{,}6(\log N+\nu)-67{,}4\log q$$
$$>99(\log N+\nu)-60{,}6(\log N+\nu)-67{,}4\log 99\nu^2a_1-67{,}4\log(\log N+\nu)$$
$$>38{,}4(\log N+\nu)-67{,}4\log 99e^2\nu^2a_1-\tfrac{67{,}4}{15}(\log N+\nu)$$
$$>33{,}9\log\frac{N}{(99e^2\nu^2a_1)^2}+33{,}9\nu>30\nu.$$

On the other hand, by Lemma 3

$$\log C<\tfrac{5}{2}\nu\log\nu+\tfrac{1}{2}\log|D|<\tfrac{5}{2}\nu\log\nu+\tfrac{1}{2}\nu^2a\leqslant\tfrac{1}{2}\nu^2(a_1+2).$$

It follows from (79), (80) and (81) that

$$q^2-40{,}4\nu cq(\nu\log 2Hq-\tfrac{2}{3}\log|\eta_1|+\tfrac{4}{3}\log q+\tfrac{1}{4}\nu)-9\nu\log C$$
$$>67\nu^2a_1\cdot30\nu^3a_1-5\nu^3(a_1+2)\geqslant5\nu^3(400\nu^2a_1^2-a_1-2)>0.$$

Since the inequality (59) is satisfied we infer by Lemma 8 and (76) that

$$(82)\qquad \log\left|\frac{\eta_2}{\eta_1}-\frac{n_2}{n_1}\right|\geqslant-10\nu cq^2\geqslant-99\cdot10^3\nu^5a_1^3(\log N+\nu)^2.$$

Since

$$|e^{i\vartheta}-1|\geqslant2\left\|\frac{\vartheta}{2\pi}\right\|\qquad(\vartheta\text{ real})$$

and

$$ik\frac{|u|+|v|}{(u,v)}(n\arg\alpha-m\arg\beta)\equiv\pm\frac{n_1}{7}\eta_2\pmod{2\pi i}$$

we get from (77), (78) and (82)

$$\log|\alpha^n-\beta^m|=\log|\exp\{i(n\arg\alpha-m\arg\beta)\}-1|$$
$$\geqslant\log2\left\|\frac{n\arg\alpha-m\arg\beta}{2\pi}\right\|$$
$$\geqslant\log\frac{2(u,v)}{k(|u|+|v|)}\left\|\frac{n_1}{7}\cdot\frac{\eta_2}{\eta_1}\right\|$$
$$=-\log\frac{k(|u|+|v|)7}{2(u,v)|n_1|}+\log\left|\frac{\eta_2}{\eta_1}-\frac{n_2}{n_1}\right|$$
$$\geqslant-\log\nu^3a(2^{\nu+4}+1)-99\cdot10^3\nu^5a_1^3(\log N+\nu)^2$$
$$>-10^5\nu^5a_1^3(\log N+\nu)^2.$$

II. Suppose first that $nv_0-mu_0=0$. We have $n=ku_0$, $m=kv_0$, where k is a positive integer $\leqslant N$ and $|\alpha|^n=|\beta|^m$. On the other hand, a_2 is formed for the pair $\langle\alpha^{u_0}/\beta^{v_0},1\rangle$ in the same way as a_1 is formed for $\langle\alpha,\beta\rangle$. Therefore, by the already proved case of the theorem

$$\log|\alpha^n-\beta^m|-\max\{n\log|\alpha|,m\log|\beta|\}$$
$$=\log|(\alpha^{u_0}/\beta^{v_0})^k-1|>-10^5\nu^5a_2^3(\log N+\nu)^2.$$

Suppose now that $nv_0-mu_0\neq0$. Then, choosing the sign $\pm$ so that $v_0\pm u_0=|u_0|+|v_0|$, we have

$$n\log|\alpha|-m\log|\beta|=\pm\frac{(nv_0-mu_0)}{|u_0|+|v_0|}\log|\alpha\beta^{\pm1}|,$$

whence

$$(83)\qquad|n\log|\alpha|-m\log|\beta||\geqslant\frac{|\log|\alpha\beta^{\pm1}||}{|u_0|+|v_0|}.$$

Since $(u_0,v_0)=1$ we have by Lemma 2

$$(84)\qquad|u_0|+|v_0|\leqslant\nu_0a_0(2^{\nu_0+4}+1).$$

On the other hand by the choice of sign

$$(85)\qquad|\log|\alpha\beta^{\pm1}||=\max_{i,j=\pm1}\log|\alpha^i\beta^j|\geqslant1-\min_{i,j=\pm1}|\alpha^i\beta^j|.$$

If $1-|\alpha\beta|\neq0$ we have by Lemma 1

$$\log|1-|\alpha\beta||=\log|\alpha_0'\beta_0'-\alpha_0''\beta_0''|-\log|\alpha_0'\beta_0'|$$
$$\geqslant-(\nu_0-1)\log|\alpha_0'\beta_0'-\alpha_0''\beta_0''|-\log|\alpha_0'\beta_0'|\geqslant-\nu_0a_0-(\nu_0-1)\log2.$$

Similarly, if $1-|\alpha^i\beta^j|\neq0$

$$(86)\qquad\log|1-|\alpha^i\beta^j||\geqslant-\nu_0a_0-(\nu_0-1)\log2.$$

Since $|\alpha| \neq 1$ or $|\beta| \neq 1$ we have $1 - \min_{i,j} |\alpha^i \beta^j| > 0$ and it follows from (83), (84), (85) and (86) that

$$\log|n\log|\alpha| - m\log|\beta|| \geqslant -\nu_0 a_0 - (\nu_0 - 1)\log 2 - \log \nu_0 a_0 (2^{\nu_0+4}+1).$$

We have however the inequality for x, y positive, $x \neq y$

$$\log|x-y| - \max\{\log x, \log y\} \geqslant \min\{0, \log|\log x - \log y|\} + \log(1-1/e). \tag{87}$$

It follows hence

$$\log|\alpha^n - \beta^m| - \max\{n\log|\alpha|, m\log|\beta|\} \geqslant -\nu_0 a_0 - (\nu_0-1)\log 2 - \log \nu_0 a_0 (2^{\nu_0+4}+1) + \log(1-1/e) \geqslant -\nu_0(2a_0+5).$$

III. Since the theorem is symmetrical with respect to α^n and β^m we can assume without loss of generality that $|\log|\alpha|| \geqslant |\log|\beta||$.

The number

$$J = (\alpha_0' \beta_0'')^N (|\alpha|^n |\beta|^{-m} - 1) \neq 0$$

is an integer of R_0, $|J| < 2\exp a_0 N$ and by Lemma 1

$$\log||\alpha|^n |\beta|^{-m} - 1| \geqslant -\log|\alpha_0' \beta_0''|^N - (\nu_0-1)\log 2 - (\nu_0-1)a_0 N > -\nu_0 a_0 N - \nu_0 \log 2.$$

Similarly

$$\log||\alpha|^{-n} |\beta|^m - 1| > -\nu_0 a_0 N - \nu_0 \log 2$$

and it follows that

$$\log|\alpha^n - \beta^m| - \max\{n\log|\alpha|, m\log|\beta|\} > -\nu_0 a_0 N - \nu_0 \log 2.$$

Thus, the theorem certainly holds if

$$\nu_0 a_0 N + \nu_0 \log 2 \leqslant 5\cdot 10^6 \nu_0^7 a_0^4 (\log N + a_0 + 1 + a_0^{-1})^3$$

and we can assume that

$$N > 5\cdot 10^6 \nu_0^6 a_0^3 (\log N + a_0 + 1 + a_0^{-1})^3 - a_0^{-1}\log 2.$$

Now by Minkowski's estimation for D_0

$$\nu_0 a_0 \geqslant \frac{1}{\nu_0}\log|eD_0| \geqslant 1. \tag{88}$$

Hence

$$N > 4\cdot 10^6 \nu_0^3 (\nu_0 a_0)^3 3^3 > \exp 18,$$
$$N > 4\cdot 10^6 (\log N + a_0 + 1 + a_0^{-1})^3 > \exp 24,$$
$$\log(\log N + a_0 + 1 + a_0^{-1}) < 1 + \frac{\log N + a_0 + 1 + a_0^{-1}}{10}. \tag{89}$$

We apply Lemma 8 with R_0 instead of R and we set

$$a_1 = |\alpha|, \quad a_2 = |\beta|,$$
$$a_1' = a_0', \quad a_1'' = a_0'', \quad a_2' = \beta_0', \quad a_2'' = \beta_0'', \quad \eta_1 = \log|\alpha|, \quad \eta_2 = \log|\beta|,$$
$$n_1 = m, \quad n_2 = n, \quad q = [82\nu_0^2 a_0 (\log N + a_0 + 1 + a_0^{-1})] + 1.$$

We have

$$|\eta_1| + |\eta_2| = \log \max_{i,j=\pm 1} |\alpha|^i |\beta|^j$$

and by Lemma 1:

$$\log|\alpha||\beta| = \log\left|\frac{\alpha_0'' \beta_0''}{\alpha_0' \beta_0'}\right| \leqslant \nu_0 a_0.$$

Similarly

$$\log|\alpha^i \beta^j| \leqslant \nu_0 a_0 \quad \text{for} \quad i = \pm 1,\ j = \pm 1$$

and we obtain

$$|\eta_1| + |\eta_2| \leqslant \nu_0 a_0.$$

This and (88) implies

$$c \leqslant a_0. \tag{90}$$

It follows further that $H = N > |\eta_1|$ and

$$q > 82\nu_0^2 a_0 \cdot 27 > 2000\nu_0^2 a_0 > 1680\nu_0 c; \quad q > 82\nu_0^2, \tag{91}$$

thus the inequality (58) is satisfied. To show that q satisfies (59) we notice first that by Lemma 1

$$\log||\alpha| - 1| = \log|\alpha_0'' \beta_0' - \alpha_0' \beta_0'| - \log|\alpha_0' \beta_0'| > -(\nu_0-1)\log|\overline{\alpha_0'' \beta_0' - \alpha_0' \beta_0'}| - \log|\overline{\alpha_0' \beta_0'}| > -\nu_0 a_0 - (\nu_0-1)\log 2.$$

On the other hand, for every $x > 0$

$$|\log x| > \min\{\tfrac{1}{2}|x-1|, \log 2\},$$

thus

$$\log|\eta_1| = \log|\log|\alpha|| > \min\{\log||\alpha|-1| - \log 2, \log\log 2\} > \min(-\nu_0 a_0 - \nu_0 \log 2, \log\log 2\} = -\nu_0 a_0 - \nu_0 \log 2 \tag{92}$$

and

$$\nu_0\log 2-\tfrac{2}{3}\log|\eta_1|+\tfrac{1}{4}\nu_0 \leqslant \tfrac{5}{3}\nu_0\log 2+\tfrac{2}{3}\nu_0 a_0+\tfrac{1}{4}\nu_0 < \nu_0(a_0+1+a_0^{-1}).$$

It follows by (90) that

$$q-40{,}4\nu_0 c(\nu_0\log 2Hq-\tfrac{2}{3}\log|\eta_1|+\tfrac{4}{3}\log q+\tfrac{1}{4}\nu_0) \tag{93}$$
$$> q-40{,}4\nu_0^2 a_0(\log N+a_0+1+a_0^{-1})-94{,}3\nu_0^2 a_0\log q.$$

Since $x-t\log x$ is an increasing function for $x>t$ and by (91), $q>94{,}3\nu_0^2 a^0$ we have by (89)

$$\frac{q}{\nu_0^2 a_0}-40{,}4(\log N+a_0+1+a_0^{-1})-94{,}3\log q \tag{94}$$
$$> 82(\log N+a_0+1+a_0^{-1})-40{,}4(\log N+a_0+1+a_0^{-1})-$$
$$-94{,}3\log 82\nu_0^2 a_0-94{,}3\log(\log N+a_0+1+a_0^{-1})$$
$$> 41{,}6(\log N+a_0+1+a_0^{-1})-94{,}3\log 82e\nu_0^2 a_0-\frac{94{,}3}{10}(\log N+a_0+1+a_0^{-1})$$
$$> 31{,}5\log\frac{N}{(82e\nu_0^2 a_0)^3}+31{,}5(a_0+1) > 30(a_0+2).$$

On the other hand, by Lemma 3

$$\log C < \tfrac{5}{2}\nu_0\log\nu_0+\tfrac{1}{2}\log|D_0| < \tfrac{5}{2}\nu_0\log\nu_0+\tfrac{1}{2}\nu_0^2 a_0 \leqslant \tfrac{1}{2}\nu_0^2(a_0+2). \tag{95}$$

It follows from (88), (90), (92), (93), (94) and (95) that

$$q^2-40{,}4\nu_0 cq(\nu_0\log 2Hq-\tfrac{2}{3}\log|\eta_1|+\tfrac{4}{3}\log q+\tfrac{1}{4}\nu_0)-9\nu_0\log C$$
$$> 82\nu_0^2\cdot 30\nu_0^2 a_0(a_0+2)-5\nu_0^3(a_0+2) = 5\nu_0^3(a_0+2)(486\nu_0 a_0-1) > 0.$$

The assumptions of Lemma 8 being satisfied, we have by (90)

$$\log\left|\frac{\eta_2}{\eta_1}-\frac{n_2}{n_1}\right| > -9\nu_0 a_0(q+1)^3. \tag{96}$$

However clearly

$$q+1 \leqslant 82{,}3\nu_0^2 a_0(\log N+a_0+1+a_0^{-1}) \tag{97}$$

and it follows from (87), (92), (96) and (97) that

$$\log|\alpha^n-\beta^m|-\max\{n\log|\alpha|, m\log|\beta|\}$$
$$\geqslant \min\{0, \log|n\log|\alpha|-m\log|\beta||\}+\log(1-1/e)$$
$$\geqslant \min\{0, -9\nu_0 a_0(q+1)^3+\log n_1|\eta_1|\}+\log(1-1/e)$$
$$> -5\cdot 10^6\nu_0^7 a_0^4(\log N+a_0+1+a_0^{-1})^3, \quad \text{q. e. d.}$$

§ 3. Linear recurrences of the second order. Consider a sequence of rational integers defined by the formula

$$u_{n+1} = Pu_n-Qu_{n-1},$$

where P and Q are rational integers and

$$PQ \neq 0, \quad \Delta = P^2-4Q \neq 0, \quad u_1^2-Pu_1u_0+Qu_0^2 \neq 0. \tag{98}$$

It is well known that

$$u_n = \Omega\omega^n+\Omega'\omega'^n,$$

where ω and ω' are roots of the equation $z^2-Pz+Q=0$ and

$$\Omega = \frac{u_0\omega'-u_1}{\omega'-\omega}, \qquad \Omega' = \frac{u_1-u_0\omega}{\omega'-\omega}.$$

If Δ is positive, $|\omega|>|\omega'|$ and $k=\left[\dfrac{\log|\Omega'/\Omega|}{\log|\omega/\omega'|}\right]+1$, we have for $n\geqslant k$

$$|u_n| \geqslant |\omega|^{n-k}(|\Omega\omega^k|-|\Omega'\omega'^k|). \tag{99}$$

If Δ is negative, the problem of estimating $|u_n|$ is more complicated. We prove

THEOREM 3. *If* (98) *holds,* $\Delta<0$ *and* $P^2\neq Q, 2Q, 3Q$ *then for*

$$n > q^{11}\max\{900, 15\log Q^3(u_1^2-Pu_1u_0+Qu_0^2)\}^7$$

we have

$$|u_n| > \frac{1}{Q\sqrt{|\Delta|}}(P^2,Q)^{n/2}\exp\frac{1}{30}\sqrt[7]{\frac{n}{q^{11}}}, \tag{100}$$

where q *is any prime factor of* $Q/(P^2,Q)$.

Proof. Consider the field R generated by $\sqrt{\Delta}$ and its prime ideal $\mathfrak{q}=(q, \omega q^{-\mathrm{ord}_q P})$. Since

$$(q, \omega q^{-\mathrm{ord}_q P}, \omega' q^{-\mathrm{ord}_q P}) = 1$$

we have

$$\mathrm{norm}\,\mathfrak{q} = q, \qquad \mathrm{ord}_{\mathfrak{q}} q = 1.$$

Since norm $(u_1-u_0\omega) = u_1^2-Pu_1u_0+Qu_0^2$,

$$\mathrm{ord}_{\mathfrak{q}}(u_1-u_0\omega) \leqslant \frac{\log(u_1^2-Pu_1u_0+Qu_0^2)}{\log q} < \frac{1}{7}n.$$

We get

$$(101)\quad \operatorname{ord}_q\left(\left(\frac{\omega'^2}{(P^2,Q)}\right)^{[n/2]}-\frac{u_n(P^2,Q)^{-[n/2]}}{\omega'^{2\{n/2\}}\Omega'}\right)$$
$$=\operatorname{ord}_q\left(\frac{\Omega\omega^n}{\Omega'(P^2,Q)^{[n/2]}\omega'^{2\{n/2\}}}\right)\geqslant n-\operatorname{ord}_q(u_1-u_0\omega)>\frac{6}{7}n.$$

Since $\operatorname{ord}_q\dfrac{\omega'^2}{(P^2,Q)}=0$ it follows that

$$\frac{u_n(P^2,Q)^{-[n/2]}}{\omega'^{2\{n/2\}}\Omega'}$$

is a q-adic unit. We set in Theorem 1

$$\mathfrak{p}=\mathfrak{q},\quad \alpha=\alpha''=\frac{\omega'^2}{(P^2,Q)},\quad \beta=\frac{u_n(P^2,Q)^{-[n/2]}}{\omega'^{2\{n/2\}}\Omega'},$$
$$\alpha'=1,\quad \beta'=\omega'^{2\{n/2\}}(u_1-u_0\omega),\quad \beta''=u_n(P^2,Q)^{-[n/2]}(\omega'-\omega).$$

It follows that

$$\nu=2,\quad \mu=\frac{2}{\log q}\leqslant\frac{2}{\log 2},\quad \varrho=\varphi=1,\quad |D|\leqslant|\Delta|,$$

$$(102)\quad a=\log\max\{|eD|^{1/4},\overline{|\omega'^{2\{n/2\}}(u_1-u_0\omega)|},\overline{|u_n(P^2,Q)^{-[n/2]}(\omega'-\omega)|},$$
$$\overline{|\omega'^2(P^2,Q)^{-1}\omega'^{2\{n/2\}}(u_1-u_0\omega)|},\overline{|\omega'^2(P^2,Q)^{-1}u_n(P^2,Q)^{-[n/2]}(\omega'-\omega)|}\}$$
$$=\log\max\{Q^{1+\{n/2\}}(P^2,Q)^{-1}(u_1^2-Pu_1u_0+Qu_0^2)^{1/2},Q|u_n|(P^2,Q)^{-[n/2]-1}|\Delta|^{1/2}\}.$$

Theorem 1 gives

$$(103)\quad \operatorname{ord}_q\left(\left(\frac{\omega'^2}{(P^2,Q)}\right)^{[n/2]}-\frac{u_n(P^2,Q)^{-[n/2]}}{\omega'^{2\{n/2\}}\Omega'}\right)$$
$$<1{,}7\cdot10^9a^4q^8\left(\log\frac{n}{2}+qa+2a^{-1}\right)^3.$$

Since $n>q^{11}\cdot900^7>e^7$ we have

$$\frac{n}{(\log n)^7}>\frac{q^{11}900^7}{(11\log q+7\log900)^7}>q^4\left(\frac{900\,q}{11\log q+7\log900}\right)^7>30^7q^4.$$

If, therefore, $a<\dfrac{1}{30}\sqrt[7]{\dfrac{n}{q^{11}}}$, we would obtain

$$\log\frac{n}{2}+qa+2a^{-1}\leqslant\frac{1}{30}\sqrt[7]{\frac{n}{q^4}}+\frac{1}{30}\sqrt[7]{\frac{n}{q^4}}+2a^{-1}<\frac{1}{14}\sqrt[7]{\frac{n}{q^4}}$$

and by (101) and (103)

$$\frac{6}{7}n<1{,}7\cdot10^9\frac{1}{30^4}\left(\frac{n}{q^{11}}\right)^{4/7}\cdot q^8\frac{1}{14^3}\left(\frac{n}{q^4}\right)^{3/7}<\frac{6}{7}n,$$

which is impossible. Thus

$$a>\frac{1}{30}\sqrt[7]{\frac{n}{q^{11}}}$$

and by (102) either

$$\log\frac{Q^{1+\{n/2\}}}{(P^2,Q)}(u_1^2-Pu_1u_0+Qu_0^2)^{1/2}>\frac{1}{30}\sqrt[7]{\frac{n}{q^{11}}}$$

or

$$\log Q\sqrt{|\Delta|}\,(P^2,Q)^{-[n/2]-1}|u_n|>\frac{1}{30}\sqrt[7]{\frac{n}{q^{11}}}.$$

The first inequality is impossible in view of the condition

$$n>q^{11}\left(15\log Q^3(u_1^2-Pu_1u_0+Qu_0^2)\right)^7,$$

thus the other inequality holds and we get (100), q. e. d.

Unfortunately, Theorem 3 does not give the true order of magnitude of $\log|u_n|-\dfrac{n}{2}\log(P^2,Q)$ which is n. It is possible to obtain this true order of magnitude in the case, where ω/ω' and Ω/Ω' are multiplicatively dependent.

Indeed, we have

THEOREM 4. *If the assumptions of Theorem 3 are satisfied, $u_n\neq0$ and ω/ω' and Ω/Ω' are multiplicatively dependent then*

$$|u_n|>\frac{1}{\sqrt{|\Delta|}}|Q|^{n/2}\exp\left(-3{,}2\cdot10^6a_1^3(\log n+2)^2\right),$$

where

$$a_1=\max\{\pi,\tfrac{1}{2}\log Q(u_1^2-Pu_1u_0+Qu_0^2)\}.$$

Proof. On setting in Theorem 2:

$$\alpha=\frac{\omega}{\omega'},\quad \beta=-\frac{\Omega'}{\Omega},$$
$$\alpha'=\omega',\quad \alpha''=\omega,\quad \beta'=u_0\omega'-u_1,\quad \beta''=u_0\omega-u_1$$

we find

$$\left|\frac{u_n}{\omega'^n \Omega}\right| = \left|\frac{\omega^n}{\omega'^n} + \frac{\Omega'}{\Omega}\right| > \exp\left(-10^5 \cdot 2^5 a_1^3 (\log n + 2)^2\right),$$

where

$$a_1 = \max\left\{\pi, \log\max\left\{|eD|^{1/4}, \left(Q(u_1^2 - Pu_1u_0 + Qu_0^2)\right)^{1/2}\right\}\right\}$$

and D is the discriminant of the field generated by $\sqrt{\Delta}$. Clearly $\log|eD|^{1/4} \leqslant \max\left\{\pi, \log\left(Q(u_1^2 - Pu_1u_0 + Qu_0^2)\right)^{1/2}\right\}$ and the theorem follows.

COROLLARY 2. *If* $u_0 = 0$, $u_1 = 1$, $u_{n+1} = u_n - 2u_{n-1}$, *then for* $n > 0$

$$|u_n| > \frac{2^{n/2}}{\sqrt{7}} \exp\left(-10^8 (\log n + 2)^2\right).$$

Proof. We have here $\Omega/\Omega' = -1$ and $u_n = 0$ only for $n = 0$.

As an application of Theorem 4 we prove the following two theorems:

THEOREM 5. *If* d *is a negative odd integer* $\neq 1 - 2^k$, *the equation*

$$x^2 - d = 2^m \tag{104}$$

has at most one solution with $m > 80$, $x > 0$.

THEOREM 6. *If* d *is a negative odd integer and* p *is any prime factor of* $1 - 4d$, *then the equation*

$$x^2 - d = p^m \tag{105}$$

has at most one solution with $m > 1 + 6\dfrac{\log\log p + 10}{\log p}$, $x > 0$.

Proof of Theorem 5. It is known (cf. [12]) that if

$$\xi^2 - d = 2^{g+2} \tag{106}$$

is the solution of the equation (104) in the least positive integers, then for any solution

$$m = gn + 2, \quad |u_n| = 1,$$

where $u_0 = 0$, $u_1 = 1$, $u_{k+1} = \xi u_k - 2^g u_{k-1}$.

Moreover, it is known (ibid. p. 89) that if

$$d = 1 - 2^a A, \quad A \text{ odd}, \ A \neq 1 \tag{107}$$

then

$$n \equiv 1 \pmod{2^{g-a+1}}. \tag{108}$$

Now it follows from (106) that

$$\xi^2 - 1 = 2^a(2^{g-a+2} - A) \neq 0,$$

thus

$$2^{a-1} \leqslant \xi + 1 \leqslant 2(2^{g-a+2} - A + 1) < 2^{g-a+3}; \quad a \leqslant \frac{g+3}{2}.$$

We obtain from (108) that either $n = 1$ or

$$n > 2^{(g-1)/2}. \tag{109}$$

We apply Theorem 4 to the sequence u_n setting $P = \xi$, $Q = 2^g$. We have either

$$g < \frac{2\pi}{\log 2} < 10 \quad \text{or} \quad a_1 = \frac{\log 2}{2} g.$$

In the latter case we get from Theorem 4

$$0 = \log|u_n| > \frac{gn}{2}\log 2 - \frac{g+2}{2}\log 2 - 1{,}3 \cdot 10^5 g^3 (\log n + 2)^2$$

and

$$f(n) = n - 4 \cdot 10^5 g^2 (\log n + 2)^2 < 0. \tag{110}$$

It is easy to verify that $f(n) > 0$ implies $f'(n) > 0$, thus it follows from (109) and (110) that

$$f(2^{(g-1)/2}) < 0$$

and as the computation shows, $g \leqslant 78$. Therefore, if the equation (104) has at least two solutions, it has a solution with $m \leqslant 80$. However by the theorem of Apéry [1], the equation (104) has at most two solutions. Hence Theorem 5 follows.

Proof of Theorem 6. If $d = -1$ or -3, the equation (105) has no solutions with $m > 2$ (cf. [17] and [19]). If $d \neq -1, -3$ the ring generated by $\sqrt{d}$ has only two units: ± 1. It follows hence like for the equation (104) that if

$$\xi^2 - d = p^g$$

is the solution of (105) in the least positive integers, then for other solutions

$$m = ng, \quad |u_n| = 1,$$

where $u_0 = 0$, $u_1 = 1$, $u_{k+1} = 2\xi u_k - p^g u_{k-1}$.

Since for n even u_n is even, n must be odd and

$$u_n \equiv (2\xi)^{n-1} \equiv (4\xi^2)^{(n-1)/2} \bmod p^g. \tag{111}$$

However by the assumption

$$4\xi^2 = 4p^g + 4d \equiv 1 \bmod p, \tag{112}$$

thus $u_n \equiv 1 \bmod p$ and

$$u_n = 1. \tag{113}$$

Let $4d = 1 - p^a A$, where $(A, p) = 1$. It follows from (112) that

$$4\xi^2 - 1 = p^a(4p^{g-a} - A), \tag{114}$$

thus

$$p^a \leqslant 2\xi + 1 \leqslant 4p^{g-2} - A + 2 < p^{g-a+2}; \quad a \leqslant \frac{g+1}{2}.$$

On the other hand by (111), (113), (114)

$$\frac{n-1}{2} \equiv 0 \pmod{p^{g-a}},$$

hence either $n = 1$ or

$$n > 2p^{(g-1)/2}. \tag{115}$$

We apply Theorem 4 to the sequence u_n setting $P = 2\xi$, $Q = p^g$. We have either

$$g < \frac{2\pi}{\log p} < 1 + 6\frac{\log\log p + 10}{\log p} \quad \text{or} \quad a_1 = \frac{g}{2}\log p.$$

In the latter case we get from Theorem 4

$$0 = \log u_n > \frac{gn}{2}\log p - \frac{g}{2}\log p - 4 \cdot 10^5 (g\log p)^3 (\log n + 2)^2$$

and

$$f(n) = n - 1 - 8 \cdot 10^5 (g\log p)^2 (\log n + 2)^2 < 0. \tag{116}$$

It is easy to verify that $f(n) > 0$ implies $f'(n) > 0$, thus it follows from (115) and (116) that

$$f_1(g) = f(2p^{(g-1)/2}) < 0.$$

On the other hand

$$f_1\left(1 + 6\frac{\log\log p + 10}{\log p}\right) > 0$$

for all $p \geqslant 3$. Since $f_1(g) > 0$ implies $f_1'(g) > 0$, it follows hence that

$$g < 1 + 6\frac{\log\log p + 10}{\log p}.$$

Since by the theorem of Apéry [2] the equation (105) has at most two solutions, we reach the desired conclusion.

COROLLARY 3. *If d is a negative integer, $d \not\equiv 0 \bmod 3$, then the equation*

$$x^2 - d = 3^m \tag{117}$$

has at most one solution with $m > 56$, $x > 0$.

Proof. If the equation (117) is solvable we have $d \equiv 1 \bmod 3$ and Theorem 6 applies.

COROLLARY 4. *If d is a negative integer, p a prime factor of $1 - 4d$ and $p > 5 \cdot 10^{37}$, then the equation*

$$x^2 - d = p^m$$

has at most one solution with $m > 1$, $x > 0$.

Proof. For $p > 5 \cdot 10^{37}$ we have $1 + 6\dfrac{\log\log p + 10}{\log p} < 2$.

From this point onwards, with the exception of Theorem 8, the estimations although effective will not be given explicitly. We prove

THEOREM 7. *If the recurrence u_n satisfies the conditions* (98) *and $u_n \neq 0$, then*

$$q(u_n) > c_1\left(\log|u_n| - \frac{n}{2}\log(P^2, Q)\right)^{\delta} (\log n)^{7\delta},$$

where

$$\delta = \begin{cases} \frac{1}{12} & \text{if } \Delta \text{ is a perfect square,} \\ \frac{1}{19} & \text{otherwise} \end{cases}$$

and c_1 is an effectively computable constant > 0.

Proof. Let p be any prime factor of u_n and $\mathfrak{p}$ any of its prime ideal factors in the field R of degree ν generated by $\sqrt{\Delta}$. We prove that

$$\operatorname{ord}_{\mathfrak{p}} u_n = \frac{n}{2}\operatorname{ord}_{\mathfrak{p}}(P^2, Q) + p^{4\nu+4}(\log p)^{-7} O(\log^3 n + p^{3\nu}) \tag{118}$$

uniformly in p.

If ω/ω' is not a $\mathfrak{p}$-adic unit and say $\operatorname{ord}_{\mathfrak{p}}\omega > \operatorname{ord}_{\mathfrak{p}}\omega'$, we have

$$\operatorname{ord}_{\mathfrak{p}}\frac{Q}{(P^2, Q)} > 0, \quad \operatorname{ord}_{\mathfrak{p}}(P^2, Q) = 2\operatorname{ord}_{\mathfrak{p}} P = 2\operatorname{ord}_{\mathfrak{p}}\omega'$$

and for $n > \operatorname{ord}_{\mathfrak{p}}\Omega'/\Omega$ we obtain

$$\operatorname{ord}_{\mathfrak{p}}\Omega\omega^n - \frac{n}{2}\operatorname{ord}_{\mathfrak{p}}(P^2, Q) = \operatorname{ord}_{\mathfrak{p}}\Omega + n\operatorname{ord}_{\mathfrak{p}}\omega/\omega' \geqslant \operatorname{ord}_{\mathfrak{p}}\Omega + n > \operatorname{ord}_{\mathfrak{p}}\Omega'$$

$$= \operatorname{ord}_{\mathfrak{p}}\Omega'\omega'^n - \frac{n}{2}\operatorname{ord}_{\mathfrak{p}}(P^2, Q).$$

Hence

$$\operatorname{ord}_{\mathfrak{p}} u_n = \frac{n}{2}\operatorname{ord}_{\mathfrak{p}}(P^2, Q) + O(1).$$

If ω/ω' is a $\mathfrak{p}$-adic unit, we have

$$\operatorname{ord}_{\mathfrak{p}} \frac{\omega'^2}{(P^2, Q)} = 0$$

and

$$\operatorname{ord}_{\mathfrak{p}} u_n = \frac{n}{2}\operatorname{ord}_{\mathfrak{p}}(P^2, Q) + \operatorname{ord}_{\mathfrak{p}} \Omega + \operatorname{ord}_{\mathfrak{p}}\left(\frac{\omega^n}{\omega'^n} + \frac{\Omega'}{\Omega}\right).$$

Since $u_n \neq 0$ we have $\dfrac{\omega^n}{\omega'^n} + \dfrac{\Omega'}{\Omega} \neq 0$ and we can apply Theorem 1.

We get

$$\operatorname{ord}_{\mathfrak{p}}\left(\frac{\omega^n}{\omega'^n} + \frac{\Omega'}{\Omega}\right) \leqslant 10^6 \left(\frac{\nu}{\log p}\right)^7 a^4 p^{4\nu+4}(\log n + \nu a p^{\nu} + 2a^{-1})^3$$

where a is a constant depending only on ω/ω' and Ω'/Ω. The formula (118) follows and we infer that

$$\operatorname{ord}_p u_n = \frac{n}{2}\operatorname{ord}_p(P^2, Q) + p^{4\nu+4}(\log p)^{-7} O(\log^3 n + p^{3\nu}).$$

Hence

$$\log|u_n| = \sum_{p \leqslant q(u_n)} \log p \operatorname{ord}_p u_n$$

$$= \frac{n}{2}\log(P^2, Q) + \sum_{p \leqslant q(u_n)} p^{4\nu+4}(\log p)^{-6} O(\log^3 n + p^{3\nu}).$$

Since

$$\sum_{p \leqslant x} p^{\sigma}(\log p)^{\tau} = O\left(x^{\sigma+1}(\log x)^{\tau-1}\right) \quad (\sigma \neq 0)$$

we get

$$\log|u_n| - \frac{n}{2}\log(P^2, Q) = q(u_n)^{4\nu+5}\left(\log q(u_n)\right)^{-7} O\left(\log^3 n + q(u_n)^{3\nu}\right).$$

By (99) and Theorem 3 we have

$$\log\left(\log|u_n| - \frac{n}{2}\log(P^2, Q)\right) \approx \log n. \tag{119}$$

Therefore, there exist two positive constants c_2 and c_3 such that for any n either

$$q(u_n) > c_2\left(\log|u_n| - \frac{n}{2}\log(P^2, Q)\right)^{1/(4\nu+5)} (\log n)^{4/(4\nu+5)} = f_2(n)$$

or

$$q(u_n) > c_3\left(\log|u_n| - \frac{n}{2}\log(P^2, Q)\right)^{1/(7\nu+5)} (\log n)^{7/(7\nu+5)} = f_3(n).$$

Since by (119) $f_3(n) = O\left(f_2(n)\right)$ and since $\delta = 1/(7\nu+5)$, we get the theorem.

If ω/ω' and Ω/Ω' are multiplicatively dependent, Theorem 7 can be considerably improved. We confine ourselves to the case $\Delta > 0$ and prove

THEOREM 8. *If the recurrence u_n satisfies the conditions* (98) *and besides $\Delta > 0$, ω/ω' and Ω'/Ω are multiplicatively dependent, then*

$$q(u_n) \geqslant nv + u - 1,$$

where u, v are the least in absolute value integers satisfying

$$(\omega/\omega')^u = (-\Omega/\Omega')^v, \quad v > 0 \tag{120}$$

and we assume $n > 0$, $nv + u > 24$.

Proof. Let $(u, v) = \sigma$. Since the field R generated by $\sqrt{\Delta}$ contains no roots of unity besides ± 1 we have $\sigma = 1$ or 2. Let r and s be integers such that

$$ru - sv = \sigma.$$

It follows from (120) that

$$\left(\frac{\omega}{\omega'}\right)^{\sigma} = \left(-\frac{\Omega}{\Omega'}\right)^{rv}\left(\frac{\omega'}{\omega}\right)^{sv},$$

whence

$$\frac{\omega^2}{\omega'^2} = \left(\left(\frac{\Omega}{\Omega'}\right)^{2r}\left(\frac{\omega'}{\omega}\right)^{2s}\right)^{v/\sigma}. \tag{121}$$

We can assume without loss of generality that $|\omega| > |\omega'|$. The number $\left(\dfrac{\Omega}{\Omega'}\right)^r \left(\dfrac{\omega'}{\omega}\right)^s$ is then absolutely greater than 1.

On the other hand, it is the quotient of two rational integers or of two quadratic conjugates. Therefore, it can be represented in the form $\pm\dfrac{(L^{1/2}+K^{1/2})/2}{(L^{1/2}-K^{1/2})/2}$, where L, K are positive rational integers and $(4L, L-K) = 4$. Let

$$(L^{1/2}+K^{1/2})/2 = \alpha, \quad (L^{1/2}-K^{1/2})/2 = \beta.$$

The numbers α^2 and β^2 are relatively prime integers of the field R, rational or conjugate and positive. Also $\omega^2/(P^2,Q)$ and $\omega'^2/(P^2,Q)$ are such integers and since by (121)

$$\frac{\omega^2/(P^2,Q)}{\omega'^2/(P^2,Q)} = \left(\frac{\alpha^2}{\beta^2}\right)^{v/\sigma},$$

we get

$$\begin{aligned} &\omega^2 = (P^2,Q)\alpha^{2v/\sigma}, \quad && \omega'^2 = (P^2,Q)\beta^{2v/\sigma}, \\ &\omega = \varepsilon(P^2,Q)^{1/2}\alpha^{v/\sigma}, && \omega' = \varepsilon'(P^2,Q)^{1/2}\beta^{v/\sigma}, \end{aligned} \tag{122}$$

where ε and ε' equal ± 1.

Since

$$(\Omega^2\Delta, \Omega'^2\Delta) = \left((2u_1 - Pu_0)^2, u_1^2 - Pu_1u_0 + Qu_0^2\right) = \Delta_1$$

is a rational integer, it follows from (120) and (122) that

$$\langle \Omega(\omega-\omega'), \Omega'(\omega'-\omega)\rangle = \begin{cases} \langle \eta\Delta_1^{1/2}\alpha^{u/\sigma}, \eta'\Delta_1^{1/2}\beta^{u/\sigma}\rangle & \text{if } u \geqslant 0, \\ \langle \eta\Delta_1^{1/2}\beta^{|u|/\sigma}, \eta'\Delta_1^{1/2}\alpha^{|u|/\sigma}\rangle & \text{if } u < 0. \end{cases} \tag{123}$$

Thus we obtain

$$u_n = \eta\Delta_1^{1/2}\varepsilon^{n-1}(P^2,Q)^{(n-1)/2}(\alpha\beta)^{(|u|-u)/2\sigma}\frac{\alpha^{(nv+u)/\sigma} - \eta\eta'(\varepsilon\varepsilon')^n\beta^{(nv+u)/\sigma}}{\alpha^{v/\sigma} - \varepsilon\varepsilon'\beta^{v/\sigma}}.$$

It follows from the work of M. Ward [25] that for every $m > 12$, $\alpha^m \pm \beta^m$ has a rational prime factor (called primitive) that is relatively prime to $\alpha^k \pm \beta^k$ for each $k < m$. This prime factor is of the form $mt \pm 1$ for $\alpha^m - \beta^m$ and of the form $2mt \pm 1$, for $\alpha^m + \beta^m$.

Since $\left((nv+u)/\sigma, v/\sigma\right) = 1$, the highest common factor of

$$\alpha^{(nv+u)/\sigma} - \eta\eta'(\varepsilon\varepsilon')^n\beta^{(nv+u)/\sigma} \quad \text{and} \quad \alpha^{v/\sigma} - \varepsilon\varepsilon'\beta^{v/\sigma}$$

divides $\alpha^2 - \beta^2$. Thus, the primitive prime factor p of $\alpha^{(nv+u)/\sigma} - \eta\eta'(\varepsilon\varepsilon')^n \times \beta^{(nv+u)/\sigma}$ is relatively prime to $\alpha^{v/\sigma} - \varepsilon\varepsilon'\beta^{v/\sigma}$, we have $p \mid u_n$ and

$$q(u_n) \geqslant p \geqslant nv + u - 1,$$

except possibly if $\sigma = 2$, $\eta\eta'(\varepsilon\varepsilon')^n = 1$. In this case we have by the choice of u, v

$$\left(\frac{\omega}{\omega'}\right)^{u/2} \neq \left(-\frac{\Omega}{\Omega'}\right)^{v/2}$$

and by (122), (123)

$$(\varepsilon\varepsilon')^{u/2} \neq (\eta\eta')^{v/2}.$$

On the other hand, $\eta\eta' = (\varepsilon\varepsilon')^n$, thus

$$(\varepsilon\varepsilon')^{(nv+u)/2} \neq 1$$

and $(nv+u)/2$ is odd. The prime p being of the form $(nv+u)t/2 \pm 1$ must be at least $nv+u-1$, which completes the proof.

Remark. An analysis a little more detailed proves that the theorem remains true if $nv+u > 12$. The last inequality is best possible as the example of Fibonacci sequence shows.

§ 4. Properties of the difference $x^v - \varepsilon P_1^{n_1}P_2^{n_2}\dots P_k^{n_k}$ ($v = 2$ or 3). In this section we consider the absolute value and the greatest prime factor of the difference $x^v - \varepsilon P_1^{n_1}P_2^{n_2}\dots P_k^{n_k}$, where $v = 2$ or 3, $\varepsilon = \pm 1$ and $P_1, P_2, \dots, P_k$ are positive integers.

THEOREM 9. *If x and $n_1, n_2, \dots, n_k$ are positive integers and $x^v - P_1^{n_1}P_2^{n_2}\dots P_k^{n_k} \neq 0$, then*

$$|x^v - P_1^{n_1}P_2^{n_2}\dots P_k^{n_k}| > \exp\left(c_4(\log\max\{x^v, P_1^{n_1}P_2^{n_2}\dots P_k^{n_k}\})^{1/7}\right), \tag{124}$$

where c_4 is a positive computable constant depending only on $v, P_1, P_2, \dots, P_k$.

Proof. We may assume without loss of generality that $P_1, P_2, \dots, P_k$ are distinct primes. If the quotients n_i/v are integers for $i = 1, 2, \dots, k$ the inequality (124) holds with $c_4 = (v-1)/v$. If at least one n_i/v is fractional, we consider the field R generated by $\vartheta = P_1^{[n_1/v]}P_2^{[n_2/v]}\dots P_k^{[n_k/v]}$. Set

$$\sigma = (x, P_1^{[n_1/v]}\dots P_k^{[n_k/v]}), \qquad x = \sigma y, \qquad P_1^{[n_1/v]}\dots P_k^{[n_k/v]} = \sigma P_1^{m_1}P_2^{m_2}\dots P_k^{m_k}.$$

The equation

$$x^v - P_1^{n_1}\dots P_k^{n_k} = d$$

can be rewritten in the form

$$y - P_1^{m_1}\dots P_k^{m_k}\vartheta = \delta\eta^n, \tag{125}$$

where $\eta > 1$ is the fundamental unit of K and δ is a factor of $d\sigma^{-v}$ in K chosen so that

$$|d\eta|^{1/v}\sigma^{-1}\eta^{-1} < |\delta| \leqslant |d\eta|^{1/v}\sigma^{-1}. \tag{126}$$

If

$$|y - P_1^{m_1}\dots P_k^{m_k}\vartheta| \geqslant 1$$

the inequality (124) holds with $c_4 = (v-1)/v$. If

$$|y - P_1^{m_1}\dots P_k^{m_k}\vartheta| < 1$$

we have

$$M = \log\max\{x^v, P_1^{m_1}\dots P_k^{m_k}\} \leqslant v\log\sigma + c_5 \max_{1\leqslant i\leqslant k} m_i, \tag{127}$$

where c_5 like the subsequent constants depends only on $\nu, P_1, \dots, P_k$ and can be effectively computed. On the other hand

$$P_1^{m_1} \dots P_k^{m_k} |y^\nu - P_1^{m_1\nu} \dots P_k^{m_k\nu} \vartheta^\nu - (y - P_1^{m_1} \dots P_k^{m_k}\vartheta)^\nu = d\sigma^{-\nu} - \delta^\nu \eta^{\nu m} = \delta^\nu (d\sigma^{-\nu}\delta^{-\nu} - \eta^{\nu m}) \neq 0. \tag{128}$$

Since η is a unit we can apply Theorem 1 and we get

$$\operatorname{ord}_{\mathfrak{p}}(d\sigma^{-\nu}\delta^{-\nu} - \eta^{\nu m}) \leqslant c_6 a^4 (\log^3 |\nu m| + a^3), \tag{129}$$

$$0 < a \leqslant c_7 \log \max\{d\sigma^{-\nu}, |\overline{\delta}|^\nu\} \tag{130}$$

for any prime ideal $\mathfrak{p}$ of R dividing $P_1 \dots P_k$.

Since the norm of δ equals $d\sigma^{-\nu}$ it follows from (126) that

$$|d\eta|^{1/\nu} \sigma^{-1} \eta^{-1} \leqslant |\overline{\delta}| \leqslant |d\eta|^{1/\nu} \sigma^{-1},$$

whence by (125)

$$|n| \leqslant c_8 \log \max\{y, P_1^{m_1} \dots P_k^{m_k}\} \leqslant c_8 (M - \nu \log \sigma) \tag{131}$$

and by (130)

$$a \leqslant c_9 (\log c_{10} d - \nu \log \sigma). \tag{132}$$

Further by the choice of σ, if $m_i > 0$ and $\mathfrak{p} | P_i$ then $\operatorname{ord}_{\mathfrak{p}} \delta = 0$. Therefore, by (128), (129), (131), and (132)

$$\max_{1 \leqslant i \leqslant k} m_i < c_{11} (\log c_{10} d - \nu \log \sigma)^4 \left(\log^3 (M - \nu \log \sigma) + (\log c_{10} d - \nu \log c)^3\right)$$

and by (127)

$$M \leqslant c_{12} (\log c_{10} d)^4 (\log^3 M + \log^3 d).$$

Solving the last inequality with respect to d we obtain (124).

COROLLARY 5. *If ξ is any real quadratic irrationality and g any positive integer > 1, then*

$$\|\xi g^n\| > g^{-n} \exp(c_{13} \sqrt[7]{n}), \tag{133}$$

where c_{13} is a positive computable constant depending on ξ and g.

Proof. It suffices to prove the corollary for $\xi = \sqrt{P}$, where P is a positive integer. Setting in Theorem 9, $\nu = k = 2$, $P_1 = P$, $n_1 = 1$, $P_2 = g$, $n_2 = 2n$, we find

$$|x^2 - P g^{2n}| > \exp(c_4 \sqrt[7]{n}),$$

whence

$$\|\sqrt{P} g^n\| > g^{-n} \exp(c_{13} \sqrt[7]{n}).$$

If $(x, P_1 \dots P_k) = O(1)$ the greatest prime factor of $x^\nu - \varepsilon P_1^{n_1} \dots P_k^{n_k}$ tends to infinity together with $\max\{x^\nu, P_1^{n_1} \dots P_k^{n_k}\}$. However we can estimate the order of its growth only for $k \leqslant 3$. The precise formulation is given in the following

THEOREM 10. *Let x and $n_1, n_2, \dots, n_k$ be positive integers and*

$$\left| x^\nu - \varepsilon \prod_{i=1}^k P_i^{n_i} \right| > 1.$$

Under each of the following conditions:

(i) $k = 3, \nu = 2, \varepsilon = n_3 = 1, x^2 - P_1^{n_1} P_2^{n_2} P_3 < 0$ *and* $(4x^2, P_1 P_2 P_3) = P_3$;

(ii) $k = 2, \nu = 2, \varepsilon = n_2 = 1, x^2 - P_1^{n_1} P_2 < 0$ *and* $(x, P_1) = 1$;

(iii) $k = 2, n_2 = 1$ *and* $(\nu^\nu x^{\nu(\nu-1)}, P_1 P_2^{\nu-1}) = P_2^{\nu-1}$;

(iv) $k = n_1 = 1$

the following inequality holds

$$q\left(x^\nu - \varepsilon \prod_{i=1}^k P_i^{n_i}\right) > \left(\tfrac{1}{7}\delta + o(1)\right) \log\log \left| x^\nu - \varepsilon \prod_{i=1}^k P_i^{n_i} \right|,$$

where

$$\delta = \begin{cases} 2/(\nu-1) & \text{if } \varepsilon \prod_{i=1}^k P_i^{n_i} \text{ is a perfect } \nu\text{-th power,} \\ 2\nu/(\nu-1)^2 & \text{otherwise,} \end{cases}$$

and the effectively computable $o(1)$ tends to zero, when $\max\{x^\nu, \prod_{i=1}^k P_i^{n_i}\}$ tends to infinity.

LEMMA 9. *Let $d = x^\nu - \varepsilon \prod_{i=1}^k P_i^{n_i}$, R be the field generated by $d^{1/\nu}$ (real for $\nu = 3$) and D its discriminant. Under each of the conditions* (i)-(iv) *there exist integers $\alpha', \alpha'', \beta', \beta''$ of R, a root of unity $\zeta \in R$ and rational integers n, m such that*

$$d^{1/\nu} \text{ divides } P_k(\alpha'^n \beta''^m - \zeta \alpha''^n \beta'^m) \neq 0, \tag{134}$$

$$(\alpha'^n, d) \text{ divides } (P_k, d) = (\beta' \beta'' P_k, d), \tag{135}$$

$$\log \max\{|\overline{\alpha'}|, |\overline{\alpha''}|, |\overline{\beta'}|, |\overline{\beta''}|\} < c_{14} \sqrt{|D|} \log^{\nu-1} |eD|, \tag{136}$$

$$\max\{|n|, |m|\} < c_{15} \log \max\left\{x^\nu, \prod_{i=1}^k P_i^{n_i}\right\}. \tag{137}$$

Proof. (i) It follows from the equation

$$x^2 - d = P_1^{n_1} P_2^{n_2} P_3 \tag{138}$$

and the assumption $(4x^2, P_1P_2P_3) = P_3$ that

$$\frac{(x-\sqrt{d})^2}{P_3}\cdot\frac{(x+\sqrt{d})^2}{P_3} = P_1^{2n_1}P_2^{2n_2},$$

where $(x\pm\sqrt{d})^2/P_3$ are relatively prime integers of R.

Hence

$$\frac{(x-\sqrt{d})^2}{(P_3)} = \mathfrak{a}_1^{2n_1}\mathfrak{a}_2^{2n_2}, \tag{139}$$

where $\mathfrak{a}_1, \mathfrak{a}_2$ are ideals of R such that

$$N\mathfrak{a}_1 = P_1, \quad N\mathfrak{a}_2 = P_2 \quad (N \text{ denotes the absolute norm in } R). \tag{140}$$

Integral vectors $[u, v]$ such that $\mathfrak{a}_1^{2u}\mathfrak{a}_2^{2v}$ is a principal ideal (integral or fractional) form a lattice.

We choose a basis of this lattice in the form $[g_1, g_2]$, $[0, g_3]$, where

$$0 < g_1 \leqslant h(R), \quad 0 \leqslant g_2 < g_3 \leqslant h(R) \tag{141}$$

($h(R)$ is the class number of R) and we take as α'', β' any generators of $\mathfrak{a}_1^{2g_1}\mathfrak{a}_2^{2g_2}$ and $\mathfrak{a}_2^{2g_3}$, respectively. We set further

$$\alpha' = P_1^{g_1}P_2^{g_2}, \quad \beta'' = P_2^{g_3}. \tag{142}$$

Since by (139) $\mathfrak{a}_1^{2n_1}\mathfrak{a}_2^{2n_2}$ is a principal ideal there exist integers n, m such that

$$n_1 = ng_1, \quad n_2 = ng_2 + mg_3 \tag{143}$$

and since R has no non-trivial units

$$\frac{(x-\sqrt{d})^2}{P_3} = \zeta\alpha'^n\beta'^m,$$

where ζ is a root of unity contained in R.

On the other hand, by (138), (142) and (143)

$$\frac{x^2-d}{P_3} = \alpha'^n\beta'^m,$$

thus the divisibility (134) follows. Since $(P_1P_2P_3, d) = (P_3, d)$, (135) follows also. Further, by (140)

$$N\alpha'' = (N\mathfrak{a}_1)^{2g_1}(N\mathfrak{a}_2)^{2g_2} = P_1^{2g_1}P_2^{2g_2} = N\alpha',$$

$$N\beta' = (N\mathfrak{a}_2)^{2g_3} = P_2^{2g_3} = N\beta''.$$

Since $|\overline{\alpha'}| = \sqrt{N\alpha'}$, etc., we get from (141)

$$\log\max\{|\overline{\alpha'}|, |\overline{\alpha''}|, |\overline{\beta'}|, |\overline{\beta''}|\} \leqslant h(R)\log P_1P_2,$$

whence (136) follows in view of the estimation [15] ($|R|$ is the degree of R)

$$h(R) \leqslant c_{16}\sqrt{|D|}\log^{|R|-1}|D|. \tag{144}$$

Finally (141) and (143) imply (137).

(ii) It follows from the equation

$$(x-\sqrt{d})(x+\sqrt{d}) = x^2-d = P_1^{n_1}P_2 \tag{145}$$

and the assumption $(x, P_1) = 1$ that $(x-\sqrt{d}, x+\sqrt{d})^2 | 4P_2$, whence

$$(x-\sqrt{d}) = 2\mathfrak{a}_1^{n_1}\mathfrak{a}_2\mathfrak{a}_3^{-1}, \tag{146}$$

where $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ are ideals of R such that $2\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3^{-1}$ is integral and

$$N\mathfrak{a}_1 = P_1, \quad N\mathfrak{a}_2 = P_2, \quad N\mathfrak{a}_3 = 4. \tag{147}$$

Let g be the least positive exponent such that $\mathfrak{a}_1^{2g}$ is a principal ideal and let

$$n_1 = gm + r, \quad 1 \leqslant r \leqslant g. \tag{148}$$

Clearly

$$g \leqslant h(R) \tag{149}$$

and $(2\mathfrak{a}_1^r\mathfrak{a}_2\mathfrak{a}_3^{-1})^2$ is a principal ideal. We take as α'', β' any generators of $(2\mathfrak{a}_1^r\mathfrak{a}_2\mathfrak{a}_3^{-1})^2$ and $\mathfrak{a}_1^{2g}$, respectively and set

$$\alpha' = P_1^rP_2, \quad \beta'' = P_1^g, \quad n = 1. \tag{150}$$

Since R has no non-trivial units we get from (146)

$$(x-\sqrt{d})^2 = \zeta\alpha'^n\beta'^m,$$

where ζ is a root of unity contained in R. On the other hand, by (145), (148), (150)

$$x^2-d = \alpha'^n\beta'^m,$$

thus the divisibility (134) follows. Since $(P_1, d) = 1$, (135) follows also. Further, by (147)

$$N\alpha'' = 16(N\mathfrak{a}_1)^{2r}(N\mathfrak{a}_2)^2(N\mathfrak{a}_3)^{-2} = P_1^{2r}P_2^2 = N\alpha',$$

$$N\beta' = (N\mathfrak{a}_1)^{2g} = P_1^{2g} = N\beta''.$$

Since $|\overline{\alpha'}| = \sqrt{N\alpha'}$, etc. we get (136) from (148), (149) and (144). Finally (148) and (150) imply (137).

(iii)-(iv) It follows from the equation

$$x^2-d = \varepsilon P_1^{n_1}P_2$$

and the assumption $(v^v x^{v(v-1)}, P_1 P_2^{v-1}) = P_2^{v-1}$ that

$$\frac{(x-d^{1/v})^v}{P_2} \cdot \frac{(x^v-d)^v}{P_2^{v-1}(x-d^{1/v})^v} = \varepsilon^v P_1^{vn_1}, \tag{151}$$

where the factors on the left hand side are integers and are coprime unless $P_2 = n_1 = 1$ (case (iv)).

If $d^{1/v}$ is rational, we get

$$\frac{(x-d^{1/v})^v}{P_2} = \varepsilon\zeta\alpha''^{vn_1},$$

where α'' is a rational integer, ζ equals ± 1. Taking

$$\alpha' = P_1, \quad \beta' = \beta'' = 1, \quad n = n_1, \quad m = 1$$

we easily verify all the assertions of the lemma.

Assume now that $d^{1/v}$ is irrational. The case $v = 2$, $d < 0$ is obtained from (i) or (ii) on setting $P_1 = 1$. In the remaining cases R is real and has one fundamental unit $\eta > 1$. We get from (151)

$$\frac{(x-d^{1/v})^v}{(P_2)} = \mathfrak{a}^{vn_1}, \tag{152}$$

where $\mathfrak{a}$ is an ideal of R such that $N\mathfrak{a} = P_1$. Let g be the least positive exponent such that $\mathfrak{a}^{vg}$ is a principal ideal. Clearly $n_1 = gn$ with n integer and

$$g \leqslant h(R). \tag{153}$$

We choose for $\mathfrak{a}^{vg}$ a generator α'' such that

$$P_1^q \eta^{1/v-1} < |\alpha''| \leqslant P_1^q \eta^{1/v}. \tag{154}$$

It follows from (152) that

$$\frac{(x-d^{1/v})^v}{P_2} = \varepsilon\zeta\alpha''^m\eta^m, \tag{155}$$

where ζ is a root of unity contained in R, m is an integer.

We set

$$\alpha' = P_1^q, \quad \beta'' = 1, \quad \beta' = \eta$$

and we find

$$\frac{x^v-d}{P_2} = \varepsilon\alpha'^m\beta'^m.$$

Now (134) and (135) follow from (155) and the equality $(P_1P_2, d) = (P_k, d)$.

We notice further that $N\alpha'' = N\mathfrak{a}^{vg} = P_1^{vg}$ and in the case $v = 3$ the two conjugates of α have the same absolute value. Hence, (154) implies

$$|\overline{\alpha''}| \leqslant P_1^q \eta^{1/v} = P_1^{n_1/n}\eta^{1/v}. \tag{156}$$

By the theorem of Landau [15]

$$0 < c_{17} < \log|\eta| \leqslant c_{18}\sqrt{|D|}\log^{v-1}|D|, \tag{157}$$

and (136) follows by (144) and (153).

Since $0 \leqslant n \leqslant n_1$, it remains to estimate $|m|$. We have by (155)

$$|m| \leqslant \frac{n|\log|\alpha''|| + v\log|x-d^{1/v}|}{\log\eta} \leqslant \frac{nv\log|\overline{\alpha''}| + c_{19}\log\max\{x, P_1^{n_1}\}}{\log\eta}$$

and (137) follows by (156) and (157).

Proof of Theorem 10. Let d, R, D have the meaning of Lemma 9. We get from the well known formulae for the discriminant of a quadratic or purely cubic field

$$|D| \leqslant v^v\Big(\prod_{p|d} p\Big)^{v-1}.$$

The primes p dividing d have the property that $\prod_{i=1}^{k} P_i^{v\{n_i/v\}}$ is $\bmod p$ a vth power residue. The density of primes for which a given integer, not a vth power, is a vth power residue is $(v-1)/v$ for $v = 2$ or 3.

Since by the prime number theorem

$$\prod_{p \leqslant q(d)} p \leqslant \exp\{q(d) + o(q(d))\}$$

and for fixed ε and P_i's there exist only v^k possible values for $\varepsilon\prod_{i=1}^{k} P_i^{v\{n_i/v\}}$, we get

$$\prod_{p|d} p \leqslant \exp\{\delta_1 q(d) + o(q(d))\},$$

where

$$\delta_1 = \begin{cases} 1 & \text{if } \varepsilon\prod_{i=1}^{k} P_i^{n_i} \text{ is a } v\text{th power,} \\ \dfrac{v-1}{v} & \text{otherwise} \end{cases}$$

and $o(q(d))$ can be effectively computed. Hence

$$|D| \leqslant \exp\{(v-1)\,\delta_1 q(d) + o(q(d))\}. \tag{158}$$

Now, let p be any rational prime dividing $d/(P_k, d)$ and $\mathfrak{p}$ any prime ideal factor of p in R. We have by (134) and (135)

$$\text{(159)}\qquad \operatorname{ord}_{\mathfrak{p}} d^{1/p} \leqslant \operatorname{ord}_{\mathfrak{p}} P_k(\alpha'^n\beta''^m - \zeta\alpha''^n\beta'^m)$$
$$\leqslant 2\operatorname{ord}_{\mathfrak{p}} P_k + \operatorname{ord}_{\mathfrak{p}}\left(\frac{\alpha''^m}{\alpha'^m} - \zeta^{-1}\frac{\beta''^m}{\beta'^m}\right),$$

where $\alpha', \alpha'', \beta', \beta', \zeta$ and n, m are described in Lemma 9.

Since ζ is contained in R and R is of degree $\leqslant 3$ we have $\zeta^6 = 1$. If

$$\frac{\alpha''^{6n}}{\alpha'^{6n}} - \frac{\beta''^{6n}}{\beta'^{6n}} = 0,$$

it follows by Lemma 1

$$\text{(160)}\qquad \operatorname{ord}_{\mathfrak{p}}\left(\frac{\alpha''^n}{\alpha'^n} - \zeta^{-1}\frac{\beta''^m}{\beta'^m}\right) = \operatorname{ord}_{\mathfrak{p}}\left(\zeta\frac{\alpha''^n\beta'^m}{\alpha'^n\beta''^m} - 1\right) \leqslant \frac{\nu\log 2}{\log p} < c_{20}.$$

If

$$\frac{\alpha''^{6n}}{\alpha'^{6n}} - \frac{\beta''^{6m}}{\beta'^{6m}} \neq 0,$$

since β''/β' is a $\mathfrak{p}$-adic unit we have by Theorem 1

$$\text{(161)}\quad \operatorname{ord}_{\mathfrak{p}}\left(\frac{\alpha''^n}{\alpha'^n} - \zeta^{-1}\frac{\beta''^m}{\beta'^m}\right) \leqslant \operatorname{ord}_{\mathfrak{p}}\left(\frac{\alpha''^{6n}}{\alpha'^{6n}} - \frac{\beta''^{6m}}{\beta'^{6m}}\right)$$
$$< c_{21}a^4 p^{16}\left(\log^3\max(6|n|, 6|m|) + p^9 a^3\right),$$

where

$$a \leqslant \log\max\{|eD|, |\overline{\alpha'\beta'}|, |\overline{\alpha'\beta''}|, |\overline{\alpha''\beta'}|, |\overline{\alpha''\beta''}|\}.$$

It follows by (136) and (158)

$$\text{(162)}\qquad a \leqslant \exp\{\delta^{-1}q(d) + o(q(d))\}.$$

Further, by (137) and Theorem 9 we have

$$\text{(163)}\quad \log\max(6|n|, 6|m|) \leqslant c_{22} + \log\log\max\left\{x^v, \prod_{i=1}^{k} P_i^{n_i}\right\} \leqslant c_{23}\log\log|d|.$$

It follows from (159)-(163) that for each prime $p \mid d/(P_k, d)$

$$\operatorname{ord}_p d \leqslant \nu\operatorname{ord}_{\mathfrak{p}} d^{1/p}$$
$$\leqslant p^{16}\exp\{4\delta^{-1}q(d) + o(q(d))\}(\log^3\log|d| + p^9\exp\{3\delta^{-1}q(d)\})$$
$$\leqslant \exp\{4\delta^{-1}q(d) + o(q(d))\}(\log^3\log|d| + \exp\{3\delta^{-1}q(d)\}).$$

Hence

$$\log|d| \leqslant \log P_k + \sum_{p\mid d/(P_k,d)} \log p\operatorname{ord}_p d$$
$$\leqslant \exp\{4\delta^{-1}q(d) + o(q(d))\}(\log^3\log|d| + \exp\{3\delta^{-1}q(d)\}).$$

Solving this inequality with respect to $q(d)$ we obtain

$$q(d) \geqslant (\tfrac{1}{7}\delta + o(1))\log\log|d|,$$

where $o(1)$ can be effectively computed and by Theorem 9 tends to zero when $\max\{x^v, \prod_{i=1}^{k} P_i^{n_i}\}$ tends to infinity, q.e.d.

COROLLARY 6. *If $q_1, \ldots, q_i, r_1, \ldots, r_j$ are distinct primes and S_1, S_2 positive integers, each of the following Diophantine equations*

$$q_1^{y_1}q_2^{y_2}\ldots q_i^{y_i} + r_1^{z_1}r_2^{z_2}\ldots r_j^{z_j} = \begin{cases} 4S_1^{x_1}S_2^{x_2}, & \\ 2S_1^{x_1}S_2^{x_2}, & S_1S_2 \text{ odd}, \\ S_1^{x_1}S_2^{x_2}, & S_1S_2 \text{ odd or } x_2 = 1, \end{cases}$$

$$q_1^{y_1}q_2^{y_2}\ldots q_i^{y_i} - r_1^{z_1}r_2^{z_2}\ldots r_j^{z_j} = \begin{cases} 4S_1^{x_1}, & \\ 3S_1^{x_1}, & S_1 \not\equiv 0 \bmod 3, \\ 2S_1^{x_1}, & S_1 \not\equiv 0 \bmod 2, \\ S_1^{x_1}, & S_1 \not\equiv 0 \bmod 6 \text{ or } x_1 = 1 \end{cases}$$

can be solved effectively.

Proof. It follows from the identity

$$4y(S_1^{x_1}S_2^{x_2}S_3 - y) = S_1^{2x_1}S_2^{2x_2}S_3^2 - (S_1^{x_1}S_2^{x_2}S_3 - 2y)^2$$

and from Theorem 10 case (i) and (ii) that if $0 < y < S_1^{x_1}S_2^{x_2}S_3$, $(y, S_1S_2S_3) = 1$ and either $(4, S_1S_2S_3) = S_3$ or $S_3 = x_2 = 1$, then

$$q(y) + q(S_1^{x_1}S_2^{x_2}S_3 - y) > (\tfrac{2}{7} + o(1))\log\log S_1^{x_1}S_2^{x_2}S_3.$$

Similarly, it follows from the identity

$$4y(S_1^{x_1}S_2 + y) = (S_1^{x_1}S_2 + y)^2 - S_1^{2x_1}S_2^2$$

and from Theorem 10 case (iii) and (iv) with $\nu = 2$ that if $y > 0$, $(y, S_1S_2) = 1$ and either $(4, S_1S_2) = S_2$ or $S_2 = x_1 = 1$, then

$$q(y) + q(S_1^{x_1}S_2 + y) > (\tfrac{2}{7} + o(1))\log\log(S_1^{x_1}S_2^{x_2} + y).$$

In both cases $o(1)$ can be effectively computed, which implies the corollary except for the equations

$$q_1^{y_1}q_2^{y_2}\ldots q_i^{y_i} - r_1^{z_1}r_2^{z_2}\ldots r_j^{z_j} = ES_1^{x_1}, \quad E = 1 \text{ or } 3, \quad S_1 \not\equiv 0 \bmod 3.$$

In order to solve these equations we apply Theorem 10 case (iii) with $v=3, \varepsilon=-1, P_1=S_1, P_2=E\prod_{\mu=1}^{j} r_\mu^{3-3\{z_\mu/3\}}, x=\prod_{\mu=1}^{j} r_\mu^{[z_\mu/3]+1}$. We get

$$\max\{q_1,\dots,q_i,r_1,\dots,r_j\}=q(x^3+P_1^{x_1}P_2)>\left(\tfrac{1}{7}+o(1)\right)\log\log|x^3+P_1^{x_1}P_2|$$
$$>\left(\tfrac{1}{7}+o(1)\right)\log\log q_1^{y_1}\dots q_r^{y_r},$$

which permits to calculate $y_1,\dots,y_r$ since $o(1)$ is effectively computable.

§ 5. The greatest prime factor of a quadratic or cubic polynomial. One of the consequences of Theorem 10 merits to be stated as a separate theorem.

THEOREM 11. *If $v=2$ or 3, A and E are non-zero integers then*

$$\lim_{x=\infty}\frac{q(Ax^v-E)}{\log\log x}\geqslant\begin{cases}\frac{4}{7} & \text{if } v=2 \text{ and } AE \text{ is not a perfect square}\\ & \text{or } v=3 \text{ and } A^2E \text{ is a perfect cube},\\ \frac{2}{7} & \text{if } v=2 \text{ and } AE \text{ is a perfect square},\\ \frac{3}{14} & \text{if } v=3 \text{ and } A^2E \text{ is not a perfect cube}.\end{cases}$$

Proof. Since $Ax^v-E=A^{1-v}\left((Ax)^v-A^{v-1}E\right)$ we apply Theorem 10 case (iv) with $\varepsilon P_1=A^{v-1}E$ and obtain the assertion except in the case A^2E being a perfect cube. In this case we set $A^2E=F^3$ and since

$$q(y^3-A^2E)\geqslant q(y^2+Fy+F^2)=q\left((2y+F)^2+3F^2\right)$$

we apply Theorem 10 case (iv) with $\varepsilon P_1=-3F^2$.

COROLLARY 7. *If $f(x)$ is any quadratic polynomial without a double root, then*

$$\lim_{x=\infty}\frac{q(f(x))}{\log\log x}\geqslant\begin{cases}\frac{4}{7} & \text{if } f \text{ is irreducible},\\ \frac{2}{7} & \text{if } f \text{ is reducible}.\end{cases}$$

Proof is obtained by reducing $f(x)$ to the canonical form.

Theorem 11 can be improved if $v=2, E\mid 4$ or $v=3, E\mid 3$. The latter case was done by Nagell [18], cf. [19]. We prove

THEOREM 12. *If $A\neq 0$ is an integer and $E\mid 4$, then*

$$\lim_{x=\infty}\frac{q(Ax^2-E)}{\log\log x}\geqslant\begin{cases}4 & \text{if } AE \text{ is not a perfect square},\\ 2 & \text{if } AE \text{ is a perfect square}.\end{cases}$$

Proof. It is sufficient to prove the theorem for $A>0$ square-free and $(A,E)=1$. Let $Ax^2-E=d>AE^2$ and let d_0 be the square-free kernel of d. Clearly

$$d_0\leqslant\prod_{p\mid d}p. \tag{164}$$

The primes p dividing d have the property that AE is mod p a quadratic residue. If AE is not a perfect square the density of primes with that property is $1/2$, hence by the prime number theorem

$$\prod_{p\mid d}p\leqslant\exp\left\{\delta_1 q(d)+o\left(q(d)\right)\right\} \tag{165}$$

where

$$\delta_1=\begin{cases}1 & \text{if } AE \text{ is a perfect square},\\ \frac{1}{2} & \text{otherwise}.\end{cases}$$

On the other hand,

$$d=d_0d_1^2,\qquad (Ax)^2-Ad_0d_1^2=AE.$$

Since $(Ax)^2-AE>(AE)^2$, Ad_0 is not a perfect square. Moreover if $E=\pm 4$ we may assume Ad_0d_1 odd.

Let U_1, V_1 be the least positive solution of the equation

$$U^2-Ad_0V^2=AE \tag{166}$$

and consider the recurrence

$$u_n=\Omega\omega^n+\Omega'\omega'^n, \tag{167}$$

where

$$\omega=|AE|^{-1}(U_1+V_1\sqrt{Ad_0})^v,\qquad \omega'=|AE|^{-1}(U_1-V_1\sqrt{Ad_0})^v,$$
$$\Omega=(U_1+V_1\sqrt{Ad_0})/2,\qquad \Omega'=(-U_1+V_1\sqrt{Ad_0})/2$$

and $v=1$ if $AE=1$ or 4 or $E=-d_0$ or $-4d_0$, $v=2$ otherwise. It follows from Theorems 11 and 13 of [19] that if $E\mid 2$, ω is the least greater than 1 totally positive unit of the ring generated by $\sqrt{Ad_0}$ and if $E=4$, ω is the least such unit of the field R generated by $\sqrt{Ad_0}$. Hence ω does not exceed the sixth power of the fundamental unit of R. Applying (157) with $D=Ad_0$ or $4Ad_0$ we get from (164) and (165)

$$\log\omega=O(\sqrt{d_0}\log d_0)\leqslant\exp\left\{\tfrac{1}{2}\delta_1 q(d)+o\left(q(d)\right)\right\}.$$

It follows further from the quoted theorems of [19] that all the positive integers V satisfying (166) for a suitable integer U, are contained in $\{u_n\}$. Thus in particular

$$|d_1|=u_n.$$

Since $\omega/\omega'=(-\Omega/\Omega')^v$, it follows from Theorem 8 that

$$q(d)\geqslant q(d_1)\geqslant nv\qquad\text{or}\qquad 24\geqslant nv.$$

Now, by (167)

$$\log u_n = n\log\omega + O(1)$$

and we get

$$\log d = \log d_0 + 2\log|d_1| \leqslant \delta_1 q(d) + o\big(q(d)\big) + q(d)\exp\{\tfrac{1}{2}\delta_1 q(d) + o\big(q(d)\big)\}$$
$$= \exp\{\tfrac{1}{2}\delta_1 q(d) + o\big(q(d)\big)\}.$$

Solving this inequality with respect to $q(d)$ we obtain the theorem.

The theorems which follow go in the direction opposite to that of Theorems 11 and 12.

THEOREM 13. *If ν, A, E are non-zero integers, $\nu \geqslant 2$, then*

$$\overline{\lim_{x=\infty}} \frac{\log q(Ax^\nu - E)\log\log\log x}{\log|Ax^\nu - E|} \leqslant \begin{cases} e^{-\gamma}\dfrac{2\nu}{\varphi(2\nu)} & \text{if} \quad AE < -1, \\ 2e^{-\gamma} & \text{if} \quad AE = -1, \\ e^{-\gamma} & \text{if} \quad AE = 1, \\ e^{-\gamma}\dfrac{\nu}{\varphi(\nu)} & \text{if} \quad AE > 1, \end{cases}$$

where γ is Euler's constant and φ is Euler's function.

Proof. We assume without loss of generality $A > 0$, set for positive integers n:

$$x_n = \begin{cases} A^{-1}(A^{\nu-1}E)^{2n} & \text{if} \quad AE < -1, \\ 2^{2n-1} & \text{if} \quad AE = -1, \\ 2^n & \text{if} \quad AE = 1, \\ A^{-1}(A^{\nu-1}E)^n & \text{if} \quad AE > 1 \end{cases}$$

and find

$$\log\log\log x_n = \log\log n + o(1).$$

On the other hand,

$$Ax_n^\nu - E = E \times \begin{cases} (A^{\nu-1}E)^{2\nu n-1} & \text{if} \quad AE < -1, \\ (-2^\nu)^{2n-1} - 1 & \text{if} \quad AE = -1, \\ 2^{\nu n} - 1 & \text{if} \quad AE = 1, \\ (A^{\nu-1}E)^{\nu n-1} - 1 & \text{if} \quad AE > 1. \end{cases}$$

Denoting by X_δ the δth cyclotomic polynomial and by $d(\delta)$ the number of divisors of δ we have for any positive integers $g > 1$ and m

$$g^m - 1 = \prod_{\delta|m} X_\delta(g)$$

and by [3], p. 178

$$q(g^m - 1) \leqslant \max_{\delta|m}|X_\delta(g)| \leqslant \max_{\delta|m} g^{\varphi(\delta)+d(\delta)} \leqslant g^{\varphi(m)+d(m)}.$$

It follows that

$$\overline{\lim_{n=\infty}} \frac{\log q(Ax_n^\nu - E)\log\log\log x_n}{\log|Ax_n^\nu - E|} \leqslant \overline{\lim_{n=\infty}} \frac{\big(\varphi(kn-1) + d(kn-1)\big)\log\log n}{kn},$$

where $k = 2\nu$ if $AE < -1$, $k = 2$ if $AE = -1$, $k = 1$ if $AE = 1$ and $k = \nu$ if $AE > 1$.

Now, a standard argument (cf. [14], § 59) shows that

$$\overline{\lim_{n=\infty}} \frac{\varphi(kn-1)\log\log n}{kn} = e^{-\gamma}\frac{k}{\varphi(k)}.$$

Since

$$\lim_{n=\infty} \frac{d(kn-1)\log\log n}{kn} = 0$$

the theorem follows.

If $\nu = 2$, $E|4$ Theorem 13 can be improved to the following

THEOREM 14. *If A, E, r, s are integers, $Ar \neq 0$, $E|4$, then*

$$\overline{\lim_{x=\infty}} \frac{\log q\big(A(rx+s)^2 - E\big)\log\log\log x}{\log|A(rx+s)^2 - E|} < \infty.$$

Proof. We assume without loss of generality that $A > 0$, $r > 0$, $s > |E|$ and set

$$\alpha = \frac{s\sqrt{A} + \sqrt{As^2 - E}}{\sqrt{|E|}}, \qquad \beta = \frac{s\sqrt{A} - \sqrt{As^2 - E}}{\sqrt{|E|}}.$$

Then $\sqrt{A(As^2 - E)}$ generates a real quadratic field and α^2 is a unit of this field. Let l be the least positive exponent such that

$$\alpha^{2l} \equiv 1 \bmod r(\alpha + \beta).$$

We set for positive integers n

$$x_n = \frac{\sqrt{|E|}}{2r\sqrt{A}}(\alpha^{2ln+1} + \beta^{2ln+1}) - \frac{s}{r}.$$

We have $\dfrac{\sqrt{|E|}}{2r\sqrt{A}}(\alpha + \beta) = \dfrac{s}{r}$ and the quotient $\dfrac{\alpha^{2ln+1} + \beta^{2ln+1}}{\alpha + \beta}$ can be expressed rationally in terms of $(\alpha + \beta)^2 = 4As^2/E$ and $\alpha\beta = \pm 1$, thus x_n is rational. Moreover by the choice of l

$$\frac{\alpha^{2ln+1} + \beta^{2ln+1}}{\alpha + \beta} \equiv 1 \bmod r,$$

thus x_n is an integer. Since $\alpha > |\beta|$, we have

$$\log\log\log x_n = \log\log n + o(1),$$

$$\log\left(A(rx_n+s)^2-E\right) = 2ln\log\alpha + O(1).$$

On the other hand,

$$A(rx_n+s)^2-E = \frac{|E|}{4}(\alpha^{2ln+1}-\beta^{2ln+1})^2 = (As^2-E)\prod_{\substack{\delta\mid 2ln+1\\ \delta>1}} X_\delta^2(\alpha,\beta),$$

where

$$X_\delta(\alpha,\beta) = \beta^{\varphi(\delta)}X_\delta\left(\frac{\alpha}{\beta}\right).$$

Since $X_\delta(\alpha,\beta)$ can be for $\delta>2$ expressed rationally in terms of $(\alpha+\beta)^2$ and $\alpha\beta$, all factors on the right hand side are rational integers and we get

$$q\left(A(rx_n+s)^2-E\right) \leqslant \max\{q(As^2-E), \max_{\substack{\delta\mid 2ln+1\\ \delta>1}} |X_\delta(\alpha,\beta)|\}$$

$$\leqslant \max\{q(As^2-E), \alpha^{\varphi(2ln+1)+d(2ln+1)}\}.$$

It follows like in the proof of Theorem 13:

$$\varlimsup_{n=\infty}\frac{\log q\left(A(rx_n+s)^2-E\right)\log\log\log x_n}{\log\left(A(rx_n+s)^2-E\right)}$$

$$\leqslant \varlimsup_{n=\infty}\frac{\left(\varphi(2ln+1)+d(2ln+1)\right)\log\log n}{2ln} = e^{-\gamma}\frac{2l}{\varphi(2l)} < \infty,$$

q. e. d.

Theorems 13 and 14 do not say anything about $q(f(x))$ for a general quadratic polynomial $f(x)$. A much weaker but more general result is the following

THEOREM 15. *If $f(x)$ is any polynomial of degree $\nu>1$ with integer coefficients, then*

$$\varlimsup_{x=\infty}\frac{\log q(f(x))}{\log|f(x)|} \leqslant \begin{cases} \frac{1}{2}P(4) & \text{for} \quad \nu=2,\\ \frac{1}{2}P(6) & \text{for} \quad \nu=3,\\ P(\nu) & \text{for} \quad \nu>3, \end{cases}$$

where

$$P(\nu) = \prod_{i=1}^{\infty}\left(1-\frac{1}{u_i}\right), \qquad u_1 = \nu-1, \qquad u_{i+1} = u_i^2-2.$$

In the proof of this theorem we denote by S the set of all polynomials with integer coefficients and the leading coefficient positive.

LEMMA 10. *If $F(x)\in S$ is a polynomial of degree d there exists a polynomial $H(x)\in S$ of degree $d-1$ such that $F(H(x))$ has a factor $G(x)\in S$ of degree d^2-2d.*

Proof. Let $F(x) = a_0x^d+\ldots+a_d$. We set for any integer k

$$G_k(x) = x^dF\left(\frac{1}{x}-\frac{a_1}{(d-1)a_0}-k\right) = a_0\left(1-\frac{a_1}{(d-1)a_0}x-xH_k(x)\right),$$

where $H_k(x)$ is a polynomial, $H_k(0) = dk$ and if $F\left(-\frac{a_1}{(d-1)a_0}-k\right)\neq 0$, $H_k(x)$ is of degree $d-1$ with the leading coefficient

$$-a_0^{-1}F\left(-\frac{a_1}{(d-1)a_0}-k\right).$$

Clearly

$$F(H_k(x)-k) \equiv F\left(-\frac{G_k(x)}{a_0x}+\frac{1}{x}-\frac{a_1}{(d-1)a_0}-k\right) \tag{168}$$

$$\equiv F\left(\frac{1}{x}-\frac{a_1}{(d-1)a_0}-k\right) \equiv 0 \bmod G_k(x).$$

We choose k such that

$$(-1)^dF\left(-\frac{a_1}{(d-1)a_0}-k\right) > 0$$

and set

$$H(x) = H_k\left((-1)^{d-1}(d-1)^2a_0^2x\right)-k.$$

It is easy to verify that $H(x)\in S$. On the other hand, in view of (168), $F(H(x))$ is divisible by $G_k\left((-1)^{d-1}(d-1)^2a_0^2x\right)$. The complementary factor of $F(H(x))$ is of degree d^2-2d and its suitable multiple belonging to S can be taken as $G(x)$.

LEMMA 11. *If $f(x)$ satisfies the assumptions of Theorem 15, then for any positive integer n there exists a polynomial $h_n(x)\in S$ of degree $u_1u_2\ldots u_n$ such that $f(h_n(x))$ has a factor $g_n(x)\in S$ of degree $u_{n+1}+1$.*

Proof by induction with respect to n. For $n=1$ the assertion follows from Lemma 10 on setting there $F = \pm f$. Assume that $f(h_n(x))$ has a factor $g_n(x)\in S$ of degree $u_{n+1}+1$. Applying Lemma 10 with $F = g_n(x)$ we find a polynomial $H(x)\in S$ of degree u_{n+1} such that $g_n(H(x))$ has a factor $g_{n+1}(x)\in S$ of degree

$$(u_{n+1}+1)^2-2(u_{n+1}+1) = u_{n+1}^2-1 = u_{n+2}+1.$$

Clearly $g_{n+1}(x)$ is also a factor of $F\big(h_n(H(x))\big)$ and we complete the proof by taking $h_{n+1}(x) = h_n(H(x))$.

Proof of Theorem 15. It follows easily by induction that

$$u_{n+1}+1 = \nu\prod_{i=1}^{n}(u_i-1) \qquad (n = 1, 2, \ldots).$$

Hence $\dfrac{u_{n+1}+1}{\nu u_1 u_2 \ldots u_n}$ tends to $P(\nu)$ decreasing monotonically. Since $P(\nu) \geqslant P(4) = 0{,}55\ldots > \frac{1}{2}$ for $\nu > 3$, we have

$$u_{n+1}+1 > \nu u_1 \ldots u_n - u_{n+1} - 1.$$

By Gauss's Lemma we can assume that in Lemma 11 both polynomials $g_n(x)$ and $f\big(h_n(x)\big)/g_n(x)$ have integer coefficients. It follows that for $\nu > 3$

$$\begin{aligned}\varlimsup_{x=\infty}\frac{\log q\big(f(x)\big)}{\log|f(x)|} &\leqslant \varlimsup_{x=\infty}\frac{\log q\big(f\big(h_n(x)\big)\big)}{\log\big|f\big(h_n(x)\big)\big|}\\ &\leqslant \varlimsup_{x=\infty}\frac{\log\max\big\{|g_n(x)|,\ \big|f\big(h_n(x)\big)/g_n(x)\big|\big\}}{\log\big|f\big(h_n(x)\big)\big|}\\ &= \frac{\max\{u_{n+1}+1,\ \nu u_1 \ldots u_n - u_{n+1} - 1\}}{\nu u_1 u_2 \ldots u_n} = \frac{u_{n+1}+1}{\nu u_1 \ldots u_n}.\end{aligned}$$

Since the last inequality holds for every n, we get

$$\varlimsup_{x=\infty}\frac{\log q\big(f(x)\big)}{\log|f(x)|} \leqslant P(\nu) \qquad (\nu > 3).$$

It remains to consider $\nu = 2$ and $\nu = 3$. If $\nu = 2$ we have

$$f\big(x+f(x)+f\big(x+f(x)\big)\big) = f(x)\big(1+f'(x)+\tfrac{1}{2}f''(x)f(x)\big)f_1(x),$$

where $f_1(x)$ is a quartic polynomial with integer coefficients. It follows by the already proved part of the theorem

$$\varlimsup_{x=\infty}\frac{\log q\big(f_1(x)\big)}{\log|f_1(x)|} \leqslant P(4)$$

and

$$\begin{aligned}\varlimsup_{x=\infty}\frac{\log q\big(f(x)\big)}{\log|f(x)|} &\leqslant \varlimsup_{x=\infty}\frac{\log\max\big\{|f(x)|,\ \big|1+f'(x)+\tfrac{1}{2}f''(x)f(x)\big|,\ q\big(f_1(x)\big)\big\}}{\log\big|f\big(x+f(x)+f\big(x+f(x)\big)\big)\big|}\\ &\leqslant \max\{\tfrac{1}{2}, \tfrac{1}{4}, \tfrac{1}{2}P(4)\} = \tfrac{1}{2}P(4).\end{aligned}$$

If $\nu = 3$ there exists by Lemma 10 a polynomial $H(x)\in S$ such that

$$f\big(H(x)\big) = G_1(x)G_2(x),$$

where G_1, G_2 are cubic polynomials with integer coefficients. Applying again Lemma 10 with $F(x) = \pm G_1(x)$ we find a polynomial $H_1(x)\in S$ such that $G_1\big(H_1(x)\big) = G_3(x)G_4(x)$, where G_3, G_4 are cubic polynomials with integer coefficients. It follows by the already proved part of the theorem

$$\varlimsup_{x=\infty}\frac{\log q\big(G_2\big(H_1(x)\big)\big)}{\log\big|G_2\big(H_1(x)\big)\big|} \leqslant P(6)$$

and since $f\big(H\big(H_1(x)\big)\big) = G_2\big(H_1(x)\big)G_3(x)G_4(x)$

$$\begin{aligned}\varlimsup_{x=\infty}\frac{\log q\big(f(x)\big)}{\log|f(x)|} &\leqslant \varlimsup_{x=\infty}\frac{\log\max\big\{q\big(G_2\big(H_1(x)\big)\big),\ |G_3(x)|,\ |G_4(x)|\big\}}{\log\big|f\big(H\big(H_1(x)\big)\big)\big|}\\ &\leqslant \max\Big\{\frac{1}{2}P(6), \frac{1}{4}, \frac{1}{4}\Big\} = \frac{1}{2}P(6).\end{aligned}$$

This completes the proof.

The above proof of Theorem 15 suggests the following

Problem. *Does there exist for any polynomial $f(x)\in S$ and any $\varepsilon > 0$ a polynomial $h(x)\in S$ of degree d such that the degree of each irreducible factor of $f\big(h(x)\big)$ is less than εd?*

I do not know the answer to this problem even for $f(x) = 4x^2 + 4x + 9$, $\varepsilon = \frac{1}{2}$.

Added in proof. 1. The proof of Theorem 5 furnishes an effective bound for the size of all solutions of (104). Indeed, taking into account that $g \leqslant h(d)$ (the class-number of the ring generated by $\sqrt{d}$) and solving (110) for $g = 78$ we get $m \leqslant \max\{2\cdot 10^{13},\ h(d)+2\}$. A similar remarks applies to Theorem 6.

2. The argument used in the proof of Theorem 10 shows also that in the case (i) and (iii) if $P_1 = 1$ then $q(d) \geqslant (\delta + o(1))\log\log|d|$. For (iii), $\nu = 2$ it is shown by a different method as Theorem 12.

References

[1] R. Apéry, *Sur une équation diophantienne*, Comptes Rendus Paris 251 (1960), pp. 1263-1264.

[2] — *Sur une équation diophantienne*, Comptes Rendus Paris 251 (1960), pp. 1451-1452.

[3] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of $a^n - b^n$*, Ann. of Math. (2) 5 (1904), pp. 173-180.

[4] Z. I. Borevich and I. R. Shafarevich, *Number theory*, New York-London 1966.

[5] J. Browkin and A. Schinzel, *On the equation* $2^n - D = y^2$, Bull. Acad. Polon. Sci., Ser. sci. math. astr. phys. 8 (1960), pp. 311-318.

[6] J. W. S. Cassels, *An introduction to Diophantine approximation*, Cambridge 1957.

[7] — *On a class of exponential equations*, Ark. Mat. 4 (1960), pp. 231-233.

[8] P. Chowla, S. Chowla, M. Dunton, D. J. Lewis, *Diophantine equations in quadratic number fields*, Calcutta Math. Soc. Golden Jubilee Commemoration Vol. (1958/59), Part II, pp. 317-322.

[9] A. O. Gelfond, *Sur l'approximation du rapport de deux nombres algébriques au moyen de nombres algébriques* (Russian), Izv. Akad. Nauk SSSR (1939), pp. 509-518.

[10] — *Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier*, Mat. Sb. 7 (1949), pp. 7-25.

[11] — *Transcendental and algebraic numbers*, New York 1960.

[12] H. Hasse, *Über eine Diophantische Gleichung von Ramanujan-Nagell und ihre Verallgemeinerung*, Nagoya Math. J. 27 (1966), pp. 77-102.

[13] V. Jarnik, *Review of* [9], Zbl. Math. 24 (1941), pp. 251-252.

[14] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, New York 1953.

[15] — *Abschatzungen von Charaktersummen, Einheiten und Klassenzahlen*, Nachr. Göttingen (1918), pp. 79-97.

[16] K. Mahler, *Über den grössten Primteiler spezieller Polynome zweiten Grades*, Archiv. for math. naturvid. 41 Nr 6 (1935).

[17] T. Nagell, *Sur l'impossibilité de quelques équations à deux indéterminées*, Norsk Mat. Forenings Skrifter 1 Nr 13 (1923).

[18] — *Über den grössten Primteiler gewisser Polynome dritten Grades*, Math. Ann. 114 (1937), pp. 284-292.

[19] — *Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns*, Nova Acta Regiae Soc. Sc. Upsaliensis (4) 16 Nr 2 (1955).

[20] H. Rumsey Jr. and E. C. Posner, *On a class of exponential equations*, Proc. Amer. Math. Soc. 15 (1964), pp. 974-978).

[21] A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. 4 (1962), pp. 413-416.

[22] — *On the arithmetic of polynomials and some related problems*, Abstracts of Short Communications, ICM Stockholm 1962, p. 50.

[23] — *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. 11 (1965), pp. 1-34.

[24] S. B. Townes, *Notes on the Diophantine equation* $x^2 + 7 = 2^{n+2}$, Proc. Amer. Math. Soc. 13 (1962), pp. 864-869.

[25] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) 62 (1955), pp. 230-236.

[26] J. Wójcik, *Diophantine equations involving primes*, Ann. Polon. Math. 18 (1966), pp. 315-321.

Reçu par la Rédaction le 1. 2. 1967