References

[1] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque 18 (1974), Soc. Math. de France.
[2] H. Halberstam and H. E. Richert, *Sieve methods*, Academic Press, London 1974.
[3] H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Invent. Math. 47 (1978), pp. 171–188.
[4] — *Sieving limits*, Sem. Delange-Pisot-Poitou 1979/80, pp. 151–165, Birkhäuser, Boston-Basel-Stuttgart 1981.
[5] — *A new form of the error term in the linear sieve*, Acta Arith. 37 (1980), pp. 307–320.
[6] A. Selberg, *Sieve methods*, Proc. Sympos. Pure Math. 20 (1971), pp. 311–351.

ISTITUTO DI MATEMATICA
UNIVERSITÀ DI SALERNO
84 100 SALERNO, ITALY

Received on 24.2.1981
and in revised form on 12.6.1984 (1241)

ACTA ARITHMETICA
XLV (1986)

On the difference between perfect powers

by

JAN TURK (Apeldoorn)

1. Introduction. The problem whether there exists a function $\varphi\colon N\to N$ with $\lim_{t\to\infty}\varphi(t)=\infty$ such that

$$(0)\qquad |x^n-y^m|\geqslant\varphi(x^n)\quad\text{for all perfect powers } x^n\neq y^m$$

is still unsolved (see [5], p. 66). Actually, nothing beyond $|x^n-y^m|\geqslant 2$ for sufficiently large perfect powers $x^n\neq y^m$ ([14]) is known when there are no restrictions on the variables x, y, n, m other than the obvious ones $(x, y, n, m\in N,\ n\geqslant 2,\ m\geqslant 2)$.

When two of the four variables are restricted the following results have been established (see Section 4.1 for more details).

Two restricted bases: for every $x, y\in N$ there exists a (large) number $c=c(x, y)$ such that (0) holds with $\varphi(t)=t(2\log t)^{-c}$.

One restricted base and one restricted exponent: for every $x, m\in N$ with $m\geqslant 2$ there exist (small) positive numbers $\varepsilon_i=\varepsilon_i(x, m)$, $i=1, 2$, such that (0) holds with $\varphi(t)=\varepsilon_1 t^{\varepsilon_2}$.

Two restricted exponents: for every $n, m\in N$ with $n\geqslant 2$, $m\geqslant 2$ there exist (small) positive numbers $\varepsilon_i=\varepsilon_i(n, m)$, $i=3, 4$, such that (0) holds with $\varphi(t)=\varepsilon_3(\log t)^{\varepsilon_4}$.

It is the purpose of this paper to obtain functions φ for which (0) holds when only one of the variables is restricted. Our results are as follows (see Section 4.2 for more details).

One restricted base: for every $x\in N$ there exist (small) positive numbers $\delta_i=\delta_i(x)$, $i=1, 2$, such that (0) holds with $\varphi(t)=\delta_1 t^{\delta_2}$.

One restricted exponent: for every $n\in N$ with $n\geqslant 2$ there exist (small) positive numbers $\delta_i=\delta_i(n)$, $i=3, 4$, such that (0) holds with $\varphi(t)=\delta_3\exp\big(\delta_4(\log\log\log(t+16))^{1/2}\big)$.

The result for the case of one restricted base can actually be inferred from the detailed results on the case of one restricted base and one restricted exponent. The proof for the case of one restricted exponent depends on explicit bounds for the solutions m, x, y of the Diophantine equation $F(x)=ay^m$ (where $a\in Z$ and $F\in Z[X]$ are given) that we derive in Sections 2 and 3, thereby obtaining more explicit results than in [9] and [13].

The author thanks the referee for his thorough comments.

2. Bounds for the solutions of the Diophantine equation $F(x) = ay^m$, I. In this section we obtain an explicit upper bound for the exponent m for which there exist $x, y \in \boldsymbol{Z}$ with $|y| > 1$ and $F(x) = ay^m$, where $F \in \boldsymbol{Z}[X]$ and $a \in \boldsymbol{Z}$ are given with $a \neq 0$ and F having at least two distinct zeros. The existence of such a bound was proved in [9]. We use the following standard notation. The *height* $H(\alpha)$ of an algebraic number α is the height of the minimal integral polynomial that it satisfies (i.e. the maximum of the absolute values of the coefficients) and $\overline{|\alpha|}$ is the maximal absolute value of the conjugates of α. We shall repeatedly use that $H(\alpha/\beta) \leqslant 4^d \max\{\overline{|\alpha|}, \overline{|\beta|}\}^d$ for algebraic integers α and β $(\neq 0)$ with $[\boldsymbol{Q}(\alpha, \beta): \boldsymbol{Q}] \leqslant d$. See e.g. [2], p. 67. We shall also use the well known fact ([6], p. 135) that if $F \in \boldsymbol{Z}[X]$ divides $G \in \boldsymbol{Z}[X]$ then $H(F) \leqslant e^n H(G)$ if n is the degree of G. The numbers C and c in this paper may be different at each occurrence.

LEMMA 1. *Let K be a field with degree $d > 1$ over $\boldsymbol{Q}$, class number h, regulator R_0, discriminant D and rank of the group of units equal to r. Then, for certain absolute constants C, c*

(1) $$hR_0 \leqslant C|D|^{1/2}(\log|D|)^{d-1},$$

(2) $$1 \leqslant h \leqslant C|D|^{1/2}(\log|D|)^{d-1},$$

(3) *there exist independent units $\eta_1, \ldots, \eta_r$, generating a group*

$$U = \{\prod_{j=1}^{r} \eta_j^{b_j}:\ b_j \in \boldsymbol{Z}\},$$

with the following properties:

(4) *for every nonzero $\alpha \in K$ there exists an $\eta \in U$ with*

$$c_1^{-1} \leqslant \frac{|\sigma(\eta\alpha)|}{|N\alpha|^{1/d}} \leqslant c_1 \quad \textit{for all automorphisms } \sigma\colon K \to \boldsymbol{C},$$

where $c_1 = \exp(d^{Cd} R_0)$ and N denotes the norm map from K to $\boldsymbol{Q}$,

(5) $$\prod_{i=1}^{r} \log\overline{|\eta_i|} < C^d R_0,$$

(6) $$|\log|\sigma\eta_i|| < d^{Cd} R_0 \quad \textit{for } i = 1, \ldots, r \textit{ and all } \sigma\colon K \to \boldsymbol{C},$$

(7) $$\log\overline{|\eta_i|} > d^{-c} \quad \textit{for } i = 1, \ldots, r,$$

(8) *the absolute values of the elements of the inverse matrix of the $(r \times r)$-matrix $(e_i \log|\sigma_i \eta_j|)$ are bounded by $(10d)^{d/2}$. Here $\sigma_1, \ldots, \sigma_{r_1}$ are the automorphisms $\sigma\colon K \to \boldsymbol{C}$ with $\sigma(K) \subset \boldsymbol{R}$ and $\sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}$ those with $\sigma(K) \not\subset \boldsymbol{R}$ while $e_i = 1$ for $1 \leqslant i \leqslant r_1$ and $e_i = 2$ for $r_1 < i \leqslant r_1 + r_2 - 1 = r$.*

Proof of Lemma 1. See for (1): [12], Satz 1.

From (1) and the result [17] that $R_0 \geqslant 0.056$ for any K, (2) follows immediately.

For (3), (5) and (8) we refer to [12], (39) and (45). From [4] it follows that

(9) $$\overline{|\eta|} \geqslant 1 + d^{-c}$$

for every unit in K which is not a root of unity. This readily implies (7). From (7) and (5) it follows that

(10) $$\log\overline{|\eta_i|} \leqslant d^{Cd} R_0 \quad \text{for} \quad i = 1, \ldots, r.$$

Since $\sum_{\sigma: K \to \boldsymbol{C}} \log|\sigma\eta_i| = 0$ this implies (6).

Since for every nonzero $\alpha \in K$ there exist rational integers a_i with

$$\left|\sum_{i=1}^{r} a_i \log|\sigma\eta_i| - \log\frac{|\sigma\alpha|}{|N\alpha|^{1/d}}\right| \leqslant \frac{r}{2}\max_i|\log|\sigma\eta_i|| \quad \text{for } \sigma \in \{\sigma_1, \ldots, \sigma_r\}$$

we can infer (4) from (6).

LEMMA 2. *Let $\alpha_1, \ldots, \alpha_N$, where $N \geqslant 2$, be nonzero algebraic numbers with heights at most $A_1, \ldots, A_N$ $(\geqslant 4)$, respectively. Let K be the field generated over $\boldsymbol{Q}$ by $\alpha_1, \ldots, \alpha_N$ and put*

$$d = [K:\boldsymbol{Q}], \quad \Omega' = \prod_{j=1}^{N-1} \log A_j.$$

For every $B \geqslant 4$ the inequalities

$$0 < |\alpha_1^{b_1} \ldots \alpha_N^{b_N} - 1| < \tfrac{1}{2}\exp\left(-(16Nd)^{200N}\Omega' \log\Omega' \log A_N \log B\right)$$

have no solution in rational integers $b_1, \ldots, b_N$ with absolute values at most B.

Proof. See [2], Chapter 1, Theorem 2.

LEMMA 3. *In the situation of Lemma 2, let P be a prime ideal in K lying above the rational prime p, with ramification index e_p. Put*

$$g_p = [\tfrac{1}{2} + e_p/(p-1)], \quad G(P) = N_{K/\boldsymbol{Q}}(P^{g_p}) \cdot (N_{K/\boldsymbol{Q}}(P) - 1),$$

$$A = \max_j A_j, \quad C = (16(N+1)d)^{12(N+1)}, \quad T = CG(P)\Omega' \log\Omega'$$

and

$$h = [\log(T/\delta)], \quad \textit{where } 0 < \delta < 1 \textit{ is arbitrary.}$$

The inequalities

$$\infty > \operatorname{ord}_P(\alpha_1^{b_1} \ldots \alpha_{N-1}^{b_{N-1}} \alpha_N - 1) > \max\{hT \log A, \delta B\}$$

have no solution in rational integers $b_1, \ldots, b_{N-1}$ with absolute values at most B.

Proof. See [2], Chapter 2: take in Theorem 3, $b_N = 1$, $B' = 1$ then any δ with $0 < \delta < 1$ satisfies the requirements.

THEOREM 1. *Let $F \in Z[X]$ be monic with at least two distinct zeros. Let $a \in Z$ be nonzero and suppose that $F(x) = ay^m$ for certain $x, y, m \in Z$ with $|y| > 1$. Then*

$$m < Cn \log H + n^4 (\log n)^2 (C(\omega+2))^{Cd(\omega+2)} d^{Cd^2(\omega+2)} \times$$
$$\times |D|^{d(\omega+2)} (\log 3|D|)^{d^2(\omega+2)} \cdot \prod_{p|R} \log p \cdot (\log \log 3P(R))^2 \cdot \log 3|a| \cdot (\log \log 3|a|)^2$$

where the parameters have the following meaning. The C's are certain absolute constants; n is the degree of F and H the height. To define ω, R and D, let α be a zero of F, of degree d and multiplicity v, with minimum polynomial F_α. If $d \geqslant 2$ then $R := R_\alpha$, the resultant of $\frac{1}{v!}\left(\frac{d}{dx}\right)^v F(X)$ and F_α. If F has only zeros of degree $d = 1$ then let α_1 and α_2 be distinct ones and $R := R_{\alpha_1} R_{\alpha_2}$. Finally, $\omega = \omega(R)$, D is the discriminant of the field $Q(\alpha)$ and $P(R)$ denotes the largest prime dividing R if $|R| > 1$ and 1 otherwise.

Remark. The factor $\log 3|a| \cdot (\log \log 3|a|)^2$ in the bound for m may be omitted if R is replaced by aR.

The following corollary of Theorem 1 gives a bound for m in terms of the standard parameters of F, namely the degree n and the height H.

COROLLARY 1. *Let $a \in Z$ be nonzero and let $F \in Z[X]$ have at least two distinct zeros, degree n and height H. Suppose $F(x) = ay^m$ for certain $x, y \in Z$ with $|y| > 1$. Then:*

$$m < \exp\left\{\frac{Cn^5 (\log 3H)^2}{\log(n \log 3H)}\right\} \cdot \log 3|a| \cdot (\log \log 3|a|)^2,$$

where C is an absolute constant.

Proof of Theorem 1. Let α be a zero of F, with multiplicity v $(= v(\alpha))$. Put $K = Q(\alpha)$, $d = [K:Q]$ and let D be the discriminant of K, h the class number of K and O_K the ring of integers of K. We consider two cases.

First case. There exists an α with $d \geqslant 2$ (i.e. $K \neq Q$). Write

$$[x-\alpha]^v = AB^m, \tag{11}$$

where A and B are integral ideals in O_K with A m-free. Then, since $F(x) = ay^m$,

$$A = A_0 \prod_{i=1}^{s} P_i^{v_i}, \tag{12}$$

where A_0 divides $[a]$, $P_1, \ldots, P_s$ are the distinct prime ideals in O_K that divide $F^{(v)}(\alpha)/v!$ and $v_1, \ldots, v_s \in \{0, 1, \ldots, m-1\}$. It follows that

$$(x-\alpha)^{vh} = a_0 \prod_{i=1}^{s} \pi_i^{v_i} b^m,$$

where $a_0, \pi_1, \ldots, \pi_s, b$ are certain integers in O_K satisfying $Na_0 = NA_0^h$, $N\pi_i = NP_i^h$ and $Nb^m = NB^{mh}$. In view of Lemma 1 we can replace $a_0, \ldots, b$ by suitable associates (which we also call $a_0, \ldots, b$) so that:

$$(x-\alpha)^{vh} = a_0 \left(\prod_{i=1}^{s} \pi_i^{v_i}\right) b^m \prod_{j=1}^{r} \eta_j^{b_j} \tag{13}$$

where the $b_j \in Z$, the η_j satisfy the properties in Lemma 1, and

$$c_1^{-1} \leqslant \frac{|\sigma\beta|}{|N\beta|^{1/d}} \leqslant c_1 \quad \text{for all automorphisms } \sigma: K \to C, \tag{14}$$

for $\beta \in \{a_0, \pi_1, \ldots, \pi_s, b\}$, where $c_1 = \exp(d^{Cd} |D|^{1/2} (\log |D|)^{d-1})$.

Assuming that

$$|x| \geqslant x_1 := \max_\sigma |\sigma\alpha| =: \boxed{\alpha} \tag{15}$$

we have

$$|Nb^m|^{1/d} = NB^{mh/d} \leqslant |N(x-\alpha)|^{vh/d} \leqslant (2|x|)^{vh}, \tag{16}$$
$$|Na_0|^{1/d} = NA_0^{h/d} \leqslant |a|^h,$$
$$|N\pi_i|^{1/d} = NP_i^{h/d} \leqslant p_i^h,$$

where p_i is the rational prime in P_i $(1 \leqslant i \leqslant s)$.

We first show that

$$|b_j| \leqslant c_2 \log 2|x| \quad \text{for} \quad j = 1, \ldots, r, \tag{17}$$

where $c_2 \leqslant v \cdot d^{Cd} |D|^{1/2} (\log |D|)^{d-1}$.

Choose $\sigma_1, \ldots, \sigma_r$ as in (8). For $1 \leqslant i \leqslant r$ we have, from (13),

$$\sum_{j=1}^{r} b_j \log|\sigma_i \eta_j|$$
$$= vh \log|x - \sigma_i \alpha| - \sum_{t=1}^{s} v_t \log|\sigma_i \pi_t| - \log|\sigma_i a_0| - \log|\sigma_i b^m| =: \lambda_i.$$

In view of (14), (16), (11) and (12) we have, with $C_0 = \frac{\log c_1}{\log 2} + \frac{h}{d}$,

$$|\lambda_i| \leqslant vh \log 2|x| + \sum_{t=1}^{s} v_t \left(\log c_1 + \frac{h}{d} \log NP_t\right) + \left(\log c_1 + \frac{h}{d} \log NA_0\right) +$$
$$+ \left(\log c_1 + \frac{h}{d} \log NB^m\right)$$

$$\leqslant vh \log 2|x| + C_0\Big(\sum_{t=1}^{s} v_t \log NP_t + \log NA_0 + \log NB^m + 2\Big)$$

$$\leqslant vh \log 2|x| + C_0(\log N[x-\alpha]^v + 2) \leqslant c_3 \log 2|x|,$$

where $c_3 = vh + 3C_0 vd \leqslant v \cdot d^{Cd}|D|^{1/2}(\log|D|)^{d-1}$.

Using Cramer's rule to solve the b_j from $\sum_{j=1}^{r} b_j(e_i \log|\sigma_i \eta_j|) = e_i \lambda_i$ $(1 \leqslant i \leqslant r)$ we obtain, by (8), that

$$|b_j| \leqslant r(10d)^{d/2} 2c_3 \log 2|x| \leqslant c_2 \log 2|x|,$$

where $c_2 \leqslant 2c_3 d(10d)^{d/2}$, which proves (17).

Now we reduce the b_j in (13) modulo m and write:

(18) $$(x-\alpha)^{vh} = a_0 c^m \prod_{i=1}^{s} \pi_i^{v_i} \prod_{j=1}^{r} \eta_j^{\beta_j},$$

where $c = b \prod_{j=1}^{r} \eta_j^{(b_j-\beta_j)/m}$, $|\beta_j| < m$ and b_j and β_j have the same sign $(1 \leqslant j \leqslant r)$.

We show that

(19) $$\log 4\overline{|c|} \leqslant \frac{c_4}{m} \log 2|x|, \quad \text{where} \quad c_4 \leqslant n \cdot d^{Cd}|D|(\log|D|)^{2d-2},$$

provided that

(20) $$|x| \geqslant x_2 := \max_{F(\beta)=0} |\beta|.$$

For every $\sigma\colon K \to C$ we have, by (16), (14), (6) and (17),

$$\log 4|\sigma c| \leqslant \log 4|\sigma b| + \frac{1}{m}\sum_{j=1}^{r} |b_j - \beta_j|\,\big|\log|\sigma \eta_j|\big|$$

$$\leqslant \frac{vh}{m} \log 2|x| + \log 4c_1 + \frac{1}{m}\sum_{j=1}^{r} |b_j|\, d^{Cd} R_0$$

$$\leqslant \frac{vh}{m} \log 2|x| + \log 4c_1 + \frac{1}{m}(dc_2 \log 2|x|)\, d^{Cd} R_0.$$

In view of $|y| > 1$ and $F(x) = ay^m$ we have

$$m \leqslant (\log|F(x)|)/\log 2 \leqslant (n \log 2|x|)/\log 2$$

provided that (20) holds. Hence (19) holds with

$$c_4 \leqslant vh + dc_2 d^{Cd} R_0 + \frac{n}{\log 2} \log 4c_1 \leqslant n \cdot d^{Cd}|D|(\log 3|D|)^{2d-2}.$$

Now choose $\sigma\colon K \to C$, σ not the identity on K. From (18) and the conjugate equation we obtain:

(21) $$\left(\frac{x-\alpha}{x-\sigma\alpha}\right)^{vh} - 1 = \frac{a_0}{\sigma a_0}\left(\frac{c}{\sigma c}\right)^{m} \prod_{i=1}^{s}\left(\frac{\pi_i}{\sigma \pi_i}\right)^{v_i} \prod_{j=1}^{r}\left(\frac{\eta_j}{\sigma \eta_j}\right)^{\beta_j} - 1.$$

We shall apply Lemma 2 to obtain a lower bound for (the right side of) (21). Note that (the left side of) (21) is nonzero if $x \neq \sigma\alpha + (\sigma\alpha - \alpha)/(\zeta_k - 1)$, where k is any divisor of vh and ζ_k any primitive kth root of unity in the field generated by α and $\sigma\alpha$. This is certainly the case if

(22) $$|x| > x_3 := k(|\alpha| + |\sigma\alpha|).$$

To apply Lemma 2 we need upper bounds for the heights of the numbers in (21). We have

$$\log H(a_0/\sigma a_0) \leqslant d^2 \log 4\overline{|a_0|} \leqslant d^2(\log 4c_1 + h \log|a|) \leqslant c_5 \log 3|a|,$$

with $c_5 \leqslant d^{Cd}|D|^{1/2}(\log|D|)^{d-1}$, by (14) and (16) and Lemma 1.

$$\log H(c/\sigma c) \leqslant d^2 \log 4\overline{|c|} \leqslant \frac{c_6}{m} \log 2|x|,$$

with $c_6 = c_4 d^2 \leqslant n \cdot d^{Cd}|D|(\log|D|)^{2d-2}$, by (19).

$$\log H(\pi_i/\sigma\pi_i) \leqslant d^2 \log 4\overline{|\pi_i|} \leqslant d^2(\log 4c_1 + h \log p_i) \leqslant c_5 \log p_i$$

for $1 \leqslant i \leqslant s$, by (14) and (16).

$$\prod_{j=1}^{r} \log\max\{4, H(\eta_j/\sigma\eta_j)\} \leqslant \prod_{j=1}^{r} \log\max\{4, 4^d \overline{|\eta_j|}^d\} \leqslant \prod_{j=1}^{r} (d^c \log \overline{|\eta_j|})$$

$$\leqslant d^{cd} R_0 \leqslant d^{Cd}|D|^{1/2}(\log|D|)^{d-1} =: c_7,$$

by (7), (5) and (1).

The number of factors in the right side of (21) equals

$$2+s+r \leqslant 2+d\omega+d-1 \leqslant d(\omega+2), \quad \text{where} \quad \omega = \omega(R),$$
$$R = N\big(F^{(v)}(\alpha)/v!\big).$$

The field containing the algebraic integers in (21) has degree at most $d!$. Assuming (22), we apply Lemma 2 now, with $\alpha_N = c/\sigma c$. We obtain that the right side of (21) exceeds the following quantity in absolute value

$$\exp\Big(-(Cd(\omega+2)d^d)^{Cd(\omega+2)} c_5 \log(3|a|) \prod_{i=1}^{s}(c_5 \log p_i) \times$$
$$\times c_7 \log\Big(c_5 c_7 \prod_{i=1}^{s}(c_5 \log p_i) \log(3|a|)\Big) \cdot \frac{c_6}{m} \log(2|x|) \cdot \log m\Big).$$

This exceeds

$$\exp\left(-n\left(C(\omega+2)\right)^{Cd(\omega+2)} d^{Cd^2(\omega+2)} |D|^{d(\omega+2)} (\log 3|D|)^{d(d-1)(\omega+2)} \times \right.$$
$$\left. \times \log(3|a|)\cdot \log\log(3|a|)\cdot \prod_{p|R} \log p \cdot \log\log\left(3P(R)\right)\cdot \log(2|x|)\cdot(\log m/m)\right),$$

for certain large absolute constants C. On the other hand we have, provided that

(23) $$|x| \geqslant x_4 = Cv^2 h^2 (\max\{|\alpha|, |\sigma\alpha|\})^2,$$

that the left side of (21) exceeds $\exp(-\frac{1}{2}\log 2|x|)$ in absolute value: Since $|(1+\varepsilon)^t - 1| \leqslant 2t|\varepsilon|$ for $|\varepsilon| \leqslant t^{-1}$, $t \in N$, we have, provided $\left|\frac{\sigma\alpha-\alpha}{x-\sigma\alpha}\right| \leqslant (vh)^{-1}$, that

$$\left|\left(\frac{x-\alpha}{x-\sigma\alpha}\right)^{vh} - 1\right| \leqslant 2vh\left|\frac{\sigma\alpha-\alpha}{x-\sigma\alpha}\right|.$$

This is less than

$$4vh \max\{|\alpha|, |\sigma\alpha|\}/\tfrac{1}{2}|x| \leqslant 1/(2|x|)^{1/2} \quad \text{if} \quad |x| \geqslant 2|\sigma\alpha|$$

and

$$|x| \geqslant 128(vh \max\{|\alpha|, |\sigma\alpha|\})^2.$$

Combining the estimates for (21) gives

(24) $$m < n\log n\left(C(\omega+2)\right)^{Cd(\omega+2)} d^{Cd^2(\omega+2)} |D|^{d(\omega+2)} (\log 3|D|)^{d^2(\omega+2)} \times$$
$$\times (\log 3|a|)\cdot(\log\log 3|a|)^2 \cdot \prod_{p|R} \log p \cdot \left(\log\log 3P(R)\right)^2,$$

provided that (15), (20), (22) and (23) hold. To treat the remaining cases we observe that we have, trivially,

(25) $$m \leqslant \frac{\log|F(x)|}{\log 2} \leqslant \frac{\log H + n\log|2x|}{\log 2} \quad \text{for} \quad |x| \leqslant x_5 \ (\geqslant 1).$$

Take $x_5 = Cv^2 h^2 (\max_{F(\beta)=0} |\beta|)^2$. Then (15), (20), (22) and (23) hold if $|x| \geqslant x_5$.

Suppose now that $|x| < x_5$. Since $|\beta| \leqslant nH$ for every zero β of F we obtain from (25), using also that $x_5 \leqslant Cn^4|D|(\log 3|D|)^{2d} H^2$, that

(26) $$m < C(n\log n + n\log H + n\log|D| + nd\log\log 3|D|).$$

The bounds (24) and (26) are covered by the bound for m stated in Theorem 1.

Second case. All zeros of F are rational ($K = Q$, $d = D = 1$). Let α and α_2 be distinct zeros of F with multiplicities v_1 and v_2. Now we have

$$(x-\alpha_i)^{v_i} = a_i b_i^m \prod_{p|R_i} p^{v_p(i)} \quad \text{for} \quad i = 1, 2,$$

where $R_i = \prod_{\substack{F(\beta)=0 \\ \beta\neq\alpha_i}} (\beta-\alpha_i)$ and $v_p(i) \in \{0, 1, \ldots, m-1\}$, while a_i divides a, $i = 1, 2$. Let v be the least common multiple of v_1 and v_2 and $w_i := v/v_i$. Then

$$\left(\frac{x-\alpha_1}{x-\alpha_2}\right)^v - 1 = a_1^{w_1}\cdot a_2^{-w_2}\left(\frac{b_1^{w_1}}{b_2^{w_2}}\right)^m \cdot \prod_{p|R_1} p^{v_p(1)w_1} \prod_{p|R_2} p^{-v_p(2)w_2} - 1.$$

We have

$$|b_i^{w_i}| \leqslant |x-\alpha_i|^{v/m} \leqslant (2|x|)^{v/m} \quad \text{for} \quad |x| \geqslant |\alpha_i|, \quad i = 1, 2.$$

Assuming that

(23)* $$|x| \geqslant Cv^2 (\max_{F(\beta)=0} |\beta|)^2$$

we obtain from Lemma 2 (take $N = \omega+2$, $\alpha_1 = a_1^{w_1}\cdot a_2^{-w_2}$, $\alpha_N = b_1^{w_1}\cdot b_2^{-w_2}$, $B = mv$) that

(24)* $$m < v^2(\log 3v)^2\left(C(\omega+2)\right)^{C(\omega+2)} (\log 3|a|)(\log\log 3|a|)^2 \times$$
$$\times \prod_{p|R} \log p \cdot \left(\log\log 3P(R)\right)^2.$$

If (23)* does not hold, then, from (25) and $|\beta| \leqslant nH$, we have

(26)* $$m < Cn(\log v + \log nH).$$

The bounds (24)* and (26)* for m are covered by the one stated in Theorem 1.

Proof of Corollary 1. Suppose first that F is monic. Write $F = \prod_{j=1}^{t} F_j^{m_j}$, with $F_1, \ldots, F_t$ distinct, monic, irreducible in $Z[X]$ and $m_1, \ldots, m_t \in N$. Let α be a zero of F_1, so $F_1 = F_\alpha$, $m_1 = v$. Then the parameter $R = R_\alpha$ equals $R = |D(F_1)^{m_1}| \prod_{j=2}^{t} R(F_j, F_1)^{m_j}$, where $R(F, G)$ is the resultant of F and G and $D(F)$ the discriminant of $F (= R(F, F'))$. Note that every prime divisor of R divides $D(F^*)$, where $F^* = \prod_{j=1}^{t} F_j$ (this also holds when $R = R_{\alpha_1} R_{\alpha_2}$). So $\omega(R) \leqslant \omega\left(D(F^*)\right)$. Also note that $D|D(F^*)$. By simply bounding determinants we see that

$$D^* := |D(F^*)| \leqslant (n^*)^{3n^*}(H^*)^{2n^*},$$

where n^* and H^* are the degree and height of F^*. Furthermore we have

$$\omega(m) \leqslant C(\log 3m)(\log\log 3m)^{-1} \quad \text{for all} \quad m \in N.$$

Hence

$$(C(\omega+2))^{C(\omega+2)d} \leqslant (3D^*)^{Cd} \quad \text{and} \quad \Big(\prod_{p|R} \log p\Big)\cdot(\log\log 3P(R))^2 \leqslant (3D^*)^C.$$

Since d and n^* are bounded by n we obtain the following bound for m:

$$Cn \log H + c(a)\exp\Big\{\frac{Cn^3(\log nH^*)^2}{\log n + \log\log 3H^*}\Big\},$$

where $c(a) = (\log 3|a|)(\log\log 3|a|)^2$ and the C's are absolute constants. Finally we use that $H^* \leqslant e^n H$ (since $F^* | F$ and degree $F = n$) to obtain a bound

$$c(a)\exp\{Cn^3(n+\log H)^2/\log(n+\log H)\}.$$

If F is not monic, $F = a_n x^n + \ldots + a_0$, $a_n \neq 1$ and $F(x) = ay^m$ then

$$\tilde{F}(a_n x) = (a_n x)^n + \ldots + a_0 a_n^{n-1} = \tilde{a} y^m$$

with $\tilde{a} = a a_n^{n-1}$ and $\tilde{F}$ monic. Since $|a_n| \leqslant H$ it follows that the bound in Corollary 1 for m holds if we choose for C some large constant.

COROLLARY 2. *Suppose* $x^n - y^m = k$, *where* $x, y, n, m, k \in \mathbf{Z}$ *with* $k \neq 0$, $m \geqslant 2$, $n \geqslant 2$. *Then*

$$m < (n|k|)^{Cn^2(\omega(k)+3)}. \tag{27}$$

More precisely,

$$m < (n|k|)^{Cn^2(\omega_*(k)+3)}, \tag{28}$$

where $\omega_*(k)$ *is the number of distinct primes p that divide k with* $v_p(k) = v_p(x^n)$. *In particular,*

$$m < (n|k|)^{Cn^2} \quad \textit{if} \quad \gcd(x, y) = 1. \tag{29}$$

The C's denote certain absolute constants.

Proof. Let $F(X) = X^n - k$. The discriminant D of F satisfies

$$|D| = n^{n-1}|k|^n.$$

As observed in the proof of Corollary 1,

$$\omega(R) \leqslant \omega(D) = \omega(nk) \leqslant 1 + \omega(k)$$

since we may assume without loss of generality that n is prime. Now Theorem 1 gives the bound (27). To prove the more precise bound we argue as follows.

The factor $(3+\omega(k))n$ comes from the number s of distinct prime ideals $P_1, \ldots, P_s$ of bounded norm in (12) in the proof of Theorem 1. Of course $N(\prod_{i=1}^{s} P_i^{v_i})$ divides $F(x)$ and $\prod_{i=1}^{s} (NP_i)^{m-1}$ but these are useless bounds in general. However, when $F(x) = x^n - k$ we observe the following. Let $p | nk$ and suppose $v_p(k) \neq v_p(x^n)$. Then

$$v_p(F(x)) \overset{!}{=} \min\{v_p(x^n), v_p(k)\} \leqslant v_p(k)$$

so $N(\prod_{i=1}^{s}{}^* P_i^{v_i})$ divides k, where the $*$ indicates that the product is over those P_i for which $p_i \in P_i$ satisfies $v_{p_i}(k) \neq v_{p_i}(x^n)$. This gives the bound $m < (n|k|)^{Cn(n\omega_*(nk)+2)}$, where $\omega_*(nk) = \sum_{p|nk}^* 1$, summation only over those p with $v_p(x^n) = v_p(k)$. Since n is prime this gives the bound (28). Finally we note that if $\gcd(x, y) = 1$ then $\gcd(x^n, k) = 1$ so $\omega_*(k) = 0$. This gives (29).

3. Bounds for solutions of the Diophantine equation $F(x) = ay^m$, **II.** Suppose $F(x) = ay^m$ where $x, y \in \mathbf{Z}$ and F, a and m are given with $m \geqslant 3$, $a \neq 0$, F having at least two simple zeros. We shall obtain an upper bound for $|x|$ in terms of F, a and m.

A completely explicit bound was already obtained by Baker (see [1]). This bound has been improved considerably in [13], but that bound is not completely explicit. We use Sprindžuk's method to obtain a completely explicit bound.

THEOREM 2. *Let* $F \in \mathbf{Z}[X]$ *be monic with at least two simple zeros,* α_1 *and* α_2. *Let* $a \in \mathbf{Z}$ *be nonzero and let* $m \in \mathbf{Z}$ *with* $m \geqslant 3$. *Suppose* $x, y \in \mathbf{Z}$ *satisfy* $F(x) = ay^m$, *then*

$$|x| \leqslant \overline{|\alpha_1|} + \exp\{(s_1 d_1 m)^{Cs_1 d_1 m^3} |a|^{(3/2)(d_1+d_2)m(m-1)\varphi(m)} \times$$
$$\times |D_1 D_2|^{(3/4)m^3(m-1)\varphi(m)s_1 d_1} \cdot |D_1^{d_1} D_2^{d_2}|^{(3/2)m^3\varphi(m)} \cdot |R_1^{d_1} R_2^{d_2}|^{(3/2)m(m-1)^2\varphi(m)} \times$$
$$\times (1+\log|aD_1 D_2 R_1 R_2|)^{3s_1 d_1 m^2\varphi(m)}\}$$

where the parameters have the following meaning. Let $K_i = \mathbf{Q}(\alpha_i)$, f_i = *minimum polynomial of* α_i *over* $\mathbf{Z}$, D_i = *discriminant of* α_i, R_i = *resultant of* f_i *and* F/f_i, $s_i = [K_i : \mathbf{Q}]$, $d_i = [L : K_i]$, *where* $L = \mathbf{Q}(\alpha_1, \alpha_2)$, *for* $i = 1, 2$. *Finally* $\overline{|\alpha_1|}$ *is the maximum of the absolute values of the conjugates of* α_1 *and C is an absolute constant.*

COROLLARY 3. *Let* $F \in \mathbf{Z}[X]$ *have at least two simple zeros, degree n and height H. Let* $m \in \mathbf{N}$, $m \geqslant 3$ *and* $a \in \mathbf{Z}$, $a \neq 0$. *Suppose* $F(x) = ay^m$, *with* $x, y \in \mathbf{Z}$. *Then*

$$|x| < \exp\{(CH)^{6m^5n^4}(|a|(\log 3|a|)^n)^{3m^3n}\}.$$

If F is monic then $(CH)^{6m^5n^4}$ *can be replaced by* $(c^n H)^{5m^5n^3}$.

Proof of Corollary 3 from Theorem 2. Let

$$H_i = \max(H(f_i), H(F/f_i)) \quad \text{and} \quad n_i = \max(s_i, n - s_i).$$

By simply bounding determinants we see that

$$|D_i| \leqslant s_i^{3s_i} H(f_i)^{2s_i} \quad \text{and} \quad |R_i| \leqslant (n_i+1)^{2n_i} H_i^n.$$

Also note that

$$\overline{|\alpha_1|} \leqslant s_1 H(f_1), \quad s_i \leqslant n, \quad d_i \leqslant n-1, \quad H_i \leqslant e^n H, \quad \varphi(m) \leqslant m.$$

First suppose F is monic. Using the above we infer from Theorem 2 that

$$|x| \leqslant \exp\{(C^n H)^{5m^5n^3} (|a| (\log 3|a|)^n)^{3m^3n}\}$$

for some absolute constant C. To cover the cases F not monic it is sufficient to replace in the above bound H by H^n and a by aH^{n-1}. This gives the announced bound (with some larger C).

For the proof of Theorem 2 we need, besides Lemma 1 and Lemma 2 of Section 1, the following lemma (cf. [7], Lemma 6).

LEMMA 4. *Let K be a field and U a group of units in K as in Lemma 1. Let α, β, γ be nonzero algebraic integers in K. Let $H \geqslant 3$ be an upper bound for the heights of α, β and γ. Then the solutions of*

$$\alpha x + \beta y = \gamma$$

with $x, y \in U$ satisfy

$$\max\{\overline{|x|}, \overline{|y|}\} \leqslant \exp\big(d^{Cd} R_0^2 (\log R_0)^2 \log H \log\log H\big)$$

for some absolute constant C.

Proof. Write $x = \eta_1^{x_1} \ldots \eta_r^{x_r}$ and $y = \eta_1^{y_1} \ldots \eta_r^{y_r}$, then we have

$$\alpha\eta_1^{x_1} \ldots \eta_r^{x_r} + \beta\eta_1^{y_1} \ldots \eta_r^{y_r} = \gamma.$$

Put $X = \max\{|x_i|, 2\}$, $Y = \max\{|y_i|, 2\}$ and $Z = \max\{|x_i - y_i|, 2\}$. For every isomorphism $\sigma\colon K \to \mathbf{C}$ we have:

$$-\frac{\sigma\alpha}{\sigma\beta} \sigma(\eta_1)^{x_1-y_1} \ldots (\sigma\eta_r)^{x_r-y_r} - 1 = \frac{-\sigma\gamma}{\sigma\beta} (\sigma\eta_1)^{-y_1} \ldots (\sigma\eta_r)^{-y_r}. \tag{30}$$

We have

$$H\left(\frac{\sigma\alpha}{\sigma\beta}\right) = H\left(\frac{\alpha}{\beta}\right) \leqslant 4^d \max\{\overline{|\alpha|}, \overline{|\beta|}\}^d \leqslant (8^d H^d).$$

From Lemma 1 we obtain

$$\prod_{i=1}^{r} \log\max\{4, H\eta_i\} \leqslant \prod_{i=1}^{r} \log\max\{4, 4^d \overline{|\eta_i|}^d\} \leqslant \prod_{i=1}^{r} (d^C \log \overline{|\eta_i|}) \leqslant d^{Cd} R_0.$$

So by Lemma 2 the left side of (30) exceeds

$$\exp(-(2d)^{Cd} \log H \cdot R_0 \log R_0 \cdot \log Z).$$

Taking logarithms we obtain

$$-\sum_{j=1}^{r} y_j \log|\sigma\eta_j| + \log\left|\frac{\sigma\gamma}{\sigma\beta}\right| > -(2d)^{Cd} \cdot \log H \cdot R_0 \log R_0 \cdot \log Z.$$

Since $\left|\frac{\sigma\gamma}{\sigma\beta}\right| \leqslant d(4dH)^d$ we get

$$\sum_{j=1}^{r} y_j \log|\sigma\eta_j| < \Gamma \log Z, \tag{31}$$

where $\Gamma = d^{Cd} \log H \cdot R_0 \log R_0$.

From

$$\alpha\eta_1^{x_1-y_1} \ldots \eta_r^{x_r-y_r} + (-\gamma)\eta_1^{-y_1} \ldots \eta_r^{-y_r} = \beta$$

we similarly obtain

$$\sum_{j=1}^{r} (-y_j) \log|\sigma\eta_j| < \Gamma \log X. \tag{31*}$$

Writing $a_\sigma(y) = \sum_{j=1}^{r} y_j \log|\sigma\eta_j|$ we obtain from (31) and (31)* that

$$|a_\sigma(y)| < \Gamma \log\max\{X, Z\}.$$

Let (q_{ij}) be the inverse of the $(r \times r)$-matrix $(e_\sigma \log|\sigma\eta_j|)$ with $\sigma = \sigma_1, \ldots, \sigma_r$ as in (8). Then we obtain

$$|y_i| \leqslant r \cdot \max_{i,j} |q_{ij}| \cdot 2 \max_\sigma |a_\sigma(y)| \quad \text{for} \quad 1 \leqslant i \leqslant r,$$

so

$$Y = \max\{|y_i|, 2\} \leqslant (10d)^{d/2+1} 2\Gamma \log\max\{X, Z\} =: \Gamma^* \log\max\{X, Z\}.$$

Since $Z \leqslant X + Y$ we infer

$$Y < \Gamma^* \log(X+Y).$$

From $\beta y + \alpha x = \gamma$ we similarly obtain $X < \Gamma^* \log(Y+X)$. Assuming that $Y \leqslant X$ we get $X < \Gamma^* \log 2X$, hence $X < C\Gamma^* \log \Gamma^*$, so

$$Y \leqslant X < d^{Cd} \log H \log\log H \cdot R_0 (\log R_0)^2.$$

Finally,

$$\overline{|x|} \leqslant \prod_{i=1}^{r} \max\{\overline{|\eta_i|}, \overline{|\eta_i^{-1}|}\}^X \leqslant \prod_{i=1}^{r} (3\overline{|\eta_i|})^{dX},$$

which gives the assertion, by using Lemma 1 once more.

Proof of Theorem 2. The method of proof is as in [13], to which we refer for details. We have

$$x - \alpha_i = \gamma_i \xi_i^m \quad (i = 1, 2), \tag{32}$$

where $\gamma_i,\ \xi_i\in K_i$, with ξ_i integral, $g_i\gamma_i$ integral for some $g_i\in N$ with $g_i\leqslant |D_i|^{m/2}$ while $|N_{K_i}(\gamma_i)|\leqslant |a|\,|R(\alpha_i)|^{m-1}\,|D_i|$, where $R(\alpha_i)$ is the resultant of f_i and F' (so $R(\alpha_i)=D_i\,R(f_i,\,F/f_i)=D_i\,R_i$).

Put $K=Q(\alpha_1,\alpha_2,\,g_1\sqrt[m]{\gamma_1},\,g_2\sqrt[m]{\gamma_2},\,\zeta_m)$, where ζ_m is a primitive mth root of 1, and let $k=[K\colon Q]$. From (32) it follows that $\gamma_1\xi_1^m-\gamma_2\xi_2^m=\alpha_2-\alpha_1$. Write

(33) $$\beta_i=\sqrt[m]{\gamma_1}\cdot\xi_1-\sqrt[m]{\gamma_2}\cdot\xi_2\cdot\zeta_m^i,\qquad 1\leqslant i\leqslant m.$$

Since $\gamma_i\xi_i^m$ are integers also the β_i are integers. We have

$$|N_K\beta_i|^m=|N_K(\beta_1\ldots\beta_m)|=|N_F(\alpha_2-\alpha_1)|^{[K:L]}=:N_{12}^{[K:L]}.$$

By Lemma 1 there exist units $\varepsilon_i^{-1}\in U=U(K)$ such that for $\lambda_i=\beta_i\varepsilon_i^{-1}$ we have

(34) $$\overline{|\lambda_i|}\leqslant N_{12}^{[K:L]/mk}\exp(k^{Ck}R_0)\leqslant\exp\big(k^{Ck}(R_0+\log N_{12})\big).$$

From (33) with $i=1,2,3$ we get, writing $\delta_i=\varepsilon_i/\varepsilon_3$ $(i=1,2)$,

$$-\lambda_1\zeta_m\delta_1+(1+\zeta_m)\lambda_2\delta_2=\lambda_3.$$

The heights of the nonzero algebraic integers $-\lambda_1\zeta_m$, $(1+\zeta_m)\lambda_2$, λ_3 are at most

$$\{4\max_{1\leqslant i\leqslant 3}\overline{|\lambda_i|}\}^k\leqslant\exp\big(k^{Ck}(R_0+\log N_{12})\big)=:H.$$

By Lemma 4, therefore,

(35) $$\max\{\overline{|\delta_1|},\overline{|\delta_2|}\}<\exp\big(k^{Ck}R_0^2(\log R_0)^2(R_0+\log N_{12})\log(R_0+\log N_{12})\big).$$

The integers $\mu_i=\delta_i\lambda_i$ $(i=1,2)$ satisfy, by (34) and (35),

(36) $$\max\{\overline{|\mu_1|},\overline{|\mu_2|}\}<\exp\big(k^{Ck}R_0^2(\log R_0)^2(R_0+\log N_{12})\log(R_0+\log N_{12})\big).$$

Observe that

$$\gamma_1\xi_1^m=\frac{(\mu_1-\mu_2\zeta_m^{-1})^m}{(1-\zeta_m^{-1})^m}\varepsilon_3^m.$$

Recall that ε_3 is a unit in K. Hence there exists an isomorphism $\sigma\colon K\to C$ with $|\sigma\varepsilon_3|\leqslant 1$. Since $x=\alpha_1+\gamma_1\xi_1^m$ and $x\in Z$ we infer that

$$|x|=|\sigma x|\leqslant|\sigma\alpha_1|+\frac{|\sigma(\mu_1-\mu_2\zeta_m^{-1})|^m}{|\sigma(1-\zeta_m^{-1})|^m}\leqslant\overline{|\alpha_1|}+\frac{(2\max\{\overline{|\mu_1|},\overline{|\mu_2|}\})^m}{(2\sin\pi/m)^m}$$
$$\leqslant\overline{|\alpha_1|}+m^m\max\{\overline{|\mu_1|},\overline{|\mu_2|}\}^m.$$

By (36), also using $cm^{1/2}\leqslant\varphi(m)\leqslant k$,

$$|x|\leqslant\overline{|\alpha_1|}+\exp\big(k^{Ck}R_0^2(\log R_0)^2(R_0+\log N_{12})\log(R_0+\log N_{12})\big).$$

It remains to bound k, R_0 and N_{12}. We have, by Lemma 1,

$$R_0<C|D|^{1/2}(\log|D|)^{k-1}$$

hence

$$R_0\log R_0<Ck|D|^{1/2}(\log|D|)^k.$$

K is obtained from Q by adjoining the algebraic integers α_1, α_2, $g_1\sqrt[m]{\gamma_1}$, $g_2\sqrt[m]{\gamma_2}$, ζ_m. Hence D divides

$$D(\alpha_1)^{k/s_1}D(\alpha_2)^{k/s_2}m^k g_1^{k(m-1)}\big(N_{K_1}(\gamma_1)\big)^{(m-1)k/s_1t_1}m^k\times$$
$$\times g_2^{k(m-1)}\big(N_{K_2}(\gamma_2)\big)^{(m-1)k/s_2t_2}D(\zeta_m)^{k/\varphi(m)},$$

where $t_i=[K_i(\sqrt[m]{\gamma_i})\colon K_i]$, $i=1,2$. We have

$$k/t_i\leqslant s_i d_i m\varphi(m),\qquad k/s_i\leqslant d_i m^2\varphi(m).$$

Also

$$g_i\leqslant|D_i|^{m/2}\quad\text{and}\quad|D(\zeta_m)|\leqslant m^{\varphi(m)},$$

while

$$|N_{K_i}(\gamma_i)|\leqslant|a|\,|R(\alpha_i)|^{m-1}\,|D_i|.$$

Hence

$$|D|\leqslant|a|^{e_1}|D_1D_2|^{e_2}|D_1^{d_1}D_2^{d_2}|^{e_3}|R(\alpha_1)^{d_1}R(\alpha_2)^{d_2}|^{e_4}m^{e_5},$$

with

$$e_1=(d_1+d_2)m(m-1)\varphi(m),\qquad e_2=\tfrac{1}{2}m^3(m-1)\varphi(m)s_1d_1,$$
$$e_3=m(2m-1)\varphi(m),\qquad e_4=m(m-1)^2\varphi(m),\qquad e_5=3s_1d_1m^2\varphi(m).$$

In particular, $\log|D|<Cm^5s_1d_1\big(1+\log|aD_1D_2R(\alpha_1)R(\alpha_2)|\big)$. Observe that $N_{12}\leqslant\max\{R_1,D_1\}$: if $f_1\neq f_2$ then $N_{12}=R(f_1,f_2)$ which divides $R(f_1,F/f_1)=R_1$, while if $f_1=f_2$ then $N_{12}=D_1$. Noting again that $R(\alpha_i)=D_iR_i$ and combining the estimates gives the bound for $|x|$ stated in Theorem 2.

4. Lower bounds for $|x^n-y^m|$. In this section x, y, n, m are integers satisfying

(37) $$x^n\neq y^m,\quad n\geqslant 2,\quad m\geqslant 2,\quad x\geqslant 1,\quad y\geqslant 1.$$

4.1. Lower bounds for $|x^n-y^m|$ when two variables are restricted

4.1.1. *Two restricted bases.* We have

(38) $$|x^n-y^m|>x^n(\log x^n)^{-c}\quad\text{for } x,y,n,m,\text{ with (37) and } x^n>1,$$

with $c = c(x, y) = c_0 \log x^* \log y^* \log\log \min\{x^*, y^*\}$, where $x^* = \max\{x, 4\}$, $y^* = \max\{y, 4\}$ and c_0 is a (large) constant.

Since $|x^n - y^m| = x^n |y^m x^{-n} - 1|$ the lower bound (38) follows readily from Lemma 2; it was already essentially obtained in [15]. In [16] it is shown that (38) is sharp in the sense that it fails infinitely often when c is a small positive number.

4.1.2. *One restricted base and one restricted exponent.* Clearly, the cases with (y, n) restricted are similar to those with (x, m) restricted, so we may restrict our attention to these latter cases. The following inequalities (39) and (40) were obtained in [10]

(39) $\quad |x^n - y^m| > \varepsilon_1 (x^n)^{\varepsilon_2} \quad$ for x, y, n, m with (37), provided $m \geqslant 3$,

where the $\varepsilon_i := \varepsilon_i(x, m)$ are (small) positive numbers depending only on x and m.

If m is large in comparison to x then ε_1 can be taken as 1 and ε_2 close to 1:

(40) $\quad |x^n - y^m| > (x^n)^{1 - c(\log m)/m} \quad$ for x, y, n, m with (37),

where $c = c(x)$ is a (large) number depending only on x. Observe that for the cases $m = 2$, x fixed we have not given a nontrivial lower bound for $|x^n - y^m|$ yet. It was shown in [8], Theorem 9, that $|x^n - y^2| > \frac{1}{2}\exp(\delta(x)(\log x^n)^{1/7})$ for all x, y, n, $(m = 2)$ with (37), where $\delta(x)$ is a (small) positive number depending only on x. It was observed in [10] that the exponent 1/7 could be replaced by $1 - \varepsilon$ for any $\varepsilon > 0$ provided $\delta(x)$ would be replaced by a suitable $\delta(x, \varepsilon)$. Due to an improvement by van der Poorten of a p-adic analogue of Lemma 2 used by Schinzel, it is possible to prove that (39) also holds for $m = 2$, as we show now. We are grateful to T. N. Shorey for providing the basic ideas of the proof.

Proof that (39) holds for $m = 2$. Write $y^2 - x^n = k$, where $k \neq 0$. If n is even, or x is a square, then clearly $|k| > 2(x^n)^{1/2}$, so we may assume that $n = 2s+1$ is odd and that $K = \mathbf{Q}(\sqrt{x})$ is a real quadratic field. We may also assume that $|y - x^s\sqrt{x}| \leqslant 1$ (otherwise $|k| > (x^n)^{1/2}$). Let $0 < \varepsilon < 1$ be the fundamental unit in the ring of integers $O(K)$ of K and let R_0 $(= \log \varepsilon^{-1})$ be its regulator. We infer from (4), that $y - x^s\sqrt{x} = \beta\varepsilon^t$ for some $t \in \mathbf{Z}$ and some $\beta \in O(K)$ with $C_1^{-1} \leqslant |\sigma\beta| \leqslant C_1 |k|^{1/2}$ for both automorphisms $\sigma\colon K \to \mathbf{C}$, with $C_1 = \exp(c_0 R_0)$, where c_0, and subsequently c_1, c_2, c_3, c_4 are absolute constants. It follows easily that $|t| \leqslant c_1(\log y + R_0)$. Let σ be the nontrivial automorphism $\sigma\colon K \to \mathbf{C}$. We have $\sigma\beta(\sigma\varepsilon)^t - \beta\varepsilon^t = 2x^s\sqrt{x}$. Let P be a prime ideal in $O(K)$ dividing $\sqrt{x}$. Then it follows that

$$n \leqslant \operatorname{ord}_P(\sigma\beta(\sigma\varepsilon)^t - \beta\varepsilon^t) = \operatorname{ord}_P(\beta) + \operatorname{ord}_P\left(\left(\frac{\sigma\varepsilon}{\varepsilon}\right)^t \frac{\sigma\beta}{\beta} - 1\right).$$

Clearly $\operatorname{ord}_P(\beta) \leqslant c_2(\log|k| + R_0)$. We use Lemma 3 to obtain an upper bound for $\operatorname{ord}_P\left(\left(\frac{\sigma\varepsilon}{\varepsilon}\right)^t \frac{\sigma\beta}{\beta} - 1\right)$. We have $T \leqslant c_3 p^2 R_0 \log R_0$ where p is the rational prime in P, and $\log A \leqslant c_4(\log|k| + R_0)$ and let $0 < \delta < 1$ be arbitrary. From the just mentioned lemma we obtain that

$$\operatorname{ord}_P\left(\left(\frac{\sigma\varepsilon}{\varepsilon}\right)^t \frac{\sigma\beta}{\beta} - 1\right) \leqslant \delta|t| + T\log(T/\delta)\log A$$
$$\leqslant \delta c_1(\log y + R_0) + c_4 T\log(T/\delta)\cdot(\log|k| + R_0).$$

Assume now that $|k| \leqslant y^{\varkappa}$, where $0 < \varkappa < 1$. Then it follows that

$$n \leqslant (\delta c_1 + \varkappa c_5 T\log(T/\delta))\log y + (\delta c_1 + c_5 T\log(T/\delta))R_0.$$

Choosing

$$\delta = (2c_1 \log x)^{-1} \quad \text{and} \quad \varkappa = (2c_5 T\log(T/\delta)\log x)^{-1}$$

we obtain that

$$\log x^n < \log y + C_2 \quad \text{where} \quad C_2 = C_2(x) = (\delta c_1 + c_5 T\log(T/\delta))R_0 \log x.$$

Hence $|k| \geqslant y^2 - e^{C_2} y$, which exceeds $y^{\varkappa}$, provided that $y > y_0(x)$. We conclude that $|k| > y^{\varkappa}$ when $y > y_0(x)$. Since $y > (x^n)^{1/2} - 1$ this gives (39), with $\varepsilon_2 = \frac{1}{2}\varkappa$, for some suitably small $\varepsilon_1 = \varepsilon_1(x)$ to include the cases $1 \leqslant y \leqslant y_0(x)$.

Observe that the positive numbers $\varepsilon_2 = \varepsilon_2(x, m)$ in (39) are very small. Using hypergeometric functions Beukers has obtained (39) for $x = 2$, $m = 2$ with a fairly large ε_2, namely with $\varepsilon_2 = \varepsilon_2(2, 2) = 1/10$. See [3].

4.1.3. *Two restricted exponents.* We have

(41) $\quad |x^n - y^m| > \varepsilon_3(\log x^n)^{\varepsilon_4} \quad$ for x, y, n, m with (37),

with $\varepsilon_3 = \varepsilon_0^n$ and $\varepsilon_4 = (5m^5 n^3)^{-1}$, where ε_0 is a (small) positive number.

Proof of (41). If $n = m = 2$ then $|x^2 - y^2| > x > \log x^2$ so we may assume that $m \geqslant 3$. Put $F = X^n - k$, where $k = x^n - y^m$ $(\neq 0)$. From Corollary 3 we infer that $x^n < \exp((c^n|k|)^{5m^5n^3})$ for some constant c $(= \varepsilon_0^{-1})$. This gives (41).

For the case $\{n, m\} = \{2, 3\}$ one may take $\varepsilon_4 = 1 - \varepsilon$ for any $\varepsilon > 0$ in (41) (then $\varepsilon_3 = \varepsilon_3(\varepsilon) > 0$), as was proved in [18].

4.2. Lower bounds for $|x^n - y^m|$ when one variable is restricted.

4.2.1. *One restricted base.* The cases with y restricted are similar to those with x restricted, of course. When x is restricted the inequalities (39) and (40) in Section 4.1.2 immediately imply the following

(42) $\quad |x^n - y^m| > \delta_1(x^n)^{\delta_2} \quad$ for x, y, n, m with (37),

where $\delta_1 = \delta_1(x)$ and $\delta_2 = \delta_2(x)$ are (small) positive numbers depending only on x.

Proof of (42). For $i = 1, 2$ put $\delta_i(x) = \min \varepsilon_i(x, m) (< \frac{1}{2})$, where the minimum is over those $m \geq 2$ with $m/\log m \leq 2c(x)$, where $c(x)$ is the constant occurring in (40). Then (39) and (40) imply (42).

4.2.2. *One restricted exponent*. Clearly, the cases with m restricted are similar to those with n restricted. The results in Section 4.1 are not sufficient to obtain a nontrivial lower bound for $|x^n - y^m|$ when n is restricted. But we also have the following nontrivial lower bound when m is large in comparison to n.

(43) $$|x^n - y^m| > \sigma_1 \exp\left(\sigma_2 \left(\log m \log\log(m+1)\right)^{1/2}\right)$$
for x, y, n, m with (37),

where $\sigma_1 = n^{-1}$ and $\sigma_2 = \sigma_0 n^{-2}$, where σ_0 is a (small) positive number.

Proof of (43). Put $k = x^n - y^m$. Since $\omega(k) \leq C \log 3|k| \cdot (\log\log 3|k|)^{-1}$ for all nonzero integers k for some absolute constant C, it follows from Corollary 2 in Section 2 that for some constant C,

$$m < \exp\left(Cn^2 \log|nk| \log 3|k| (\log\log 3|k|)^{-1}\right).$$

This implies (43) for some small σ_0.

We note that (43) also follows from a more general result in [11] but that does not give the dependence on n. The inequality (43) enables us to prove our main result:

(44) $$|x^n - y^m| > \delta_3 \exp\left(\delta_4 (\log\log\log x^n)^{1/2}\right) \quad \text{for } x, y, n, m \text{ with (37)}$$
and $x^n \geq 16$,

where $\delta_3 = n^{-1}$ and $\delta_4 = \delta_0 n^{-1}$, with δ_0 a (small) positive number.

(45) $$|x^n - y^m| > \delta_3 (\log\log x^n)^{\delta_5} \quad \text{for } x, y, n, m \text{ with (37)},$$
$x^n \geq 4$ and $\gcd(x, y) = 1$,

where $\delta_5 = \delta_0' n^{-2}$, with δ_0' a (small) positive number.

Proof of (44) and (45). Put $x^n - y^m = k$. Combine the inequality $m < \exp(Cn^2(\log n|k|)^2)$ from the proof of (43) with the inequality from Corollary 3:

$$x^n < \exp\left((c^n|k|)^{5m^5n^3}\right).$$

This gives

$$x^n < \exp\exp\exp\left(Cn^2(\log n|k|)^2\right),$$

which implies (44).

If $\gcd(x, y) = 1$ then we have a better inequality for m: $m < (n|k|)^{Cn^2}$, by Corollary 2. This results in (44).

References

[1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Camb. Philos. Soc. 65 (1969), pp. 439–444.

[2] A. Baker and D. W. Masser, *Transcendence theory, Advances and Applications* (Proc. Conf., Univ. Cambridge, Cambridge 1976), Academic Press, London 1977.

[3] F. Beukers, *The generalized Ramanujan–Nagell equation*, Acta Arith. I: 38 (1981), pp. 389–410; II: 39 (1981), pp. 113–123.

[4] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, ibid. 18 (1971), pp. 355–369.

[5] P. Erdös and R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monographie no. 28 de l'Enseignement Mathématique, Genève 1980.

[6] A. O. Gelfond, *Transcendental and algebraic numbers*, Original Russian edition 1952, English translation, New York 1960.

[7] K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. 54 (1979), pp. 583–600.

[8] A. Schinzel, *On two theorems of Gelfond and some of their applications*, Acta Arith. 13 (1967), pp. 177–236.

[9] A. Schinzel and R. Tijdeman, *On the equation $y^m = P(x)$*, ibid. 31 (1976), pp. 199–204.

[10] T. N. Shorey and R. Tijdeman, *New applications of Diophantine approximations to Diophantine equations*, Math. Scand. 39 (1976), pp. 5–18.

[11] T. N. Shorey, *On the greatest prime factor of $ax^m + by^n$*, Acta Arith. 36 (1980), pp. 21–25.

[12] C. L. Siegel, *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. II (1969), pp. 71–86.

[13] V. G. Sprindžuk, *The arithmetic structure of integral polynomials and class numbers*, Proc. Steklov Inst. Math. 1980, Issue I, pp. 163–186.

[14] R. Tijdeman, *On the equation of Catalan*, Acta Arith. 29 (1976), pp. 197–209.

[15] — *On integers with many small prime factors*, Compositio Math. 26 (1973), pp. 319–330.

[16] — *On the maximal distance between integers composed of small primes*, ibid. 28 (1974), pp. 159–162.

[17] R. Zimmert, *Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung*, Invent. Math. 62 (1981), pp. 367–380.

[18] H. M. Stark, *Effective estimates of solutions of some diophantine equations*, Acta Arith. 24 (1973), pp. 251–259.

Received on 2.5.1983
and in revised form on 5.10.1984 (1355)