Powerfree Values of Polynomials

D.R. Heath-Brown
Mathematical Institute, Oxford

1 Introduction

Let \( f(X) \in \mathbb{Z}[X] \) be an irreducible polynomial of degree \( d \). It is conjectured that, for any integer \( k \geq 2 \), the polynomial \( f(n) \) takes infinitely many \( k \)-th power free values, providing that \( f \) satisfies the obviously necessary congruence conditions. Thus for every prime \( p \) we need to assume that there is at least one integer \( n_p \) for which \( p^k \nmid f(n_p) \). This problem appears to become harder as the degree \( d \) increases, but easier as \( k \) increases. Thus in 1933 Ricci [10] handled the case \( k \geq d \), and even proved an asymptotic formula

\[
N_{f,k}(x) \sim A(f,k)x \quad (x \to \infty)
\]

where

\[
N_{f,k}(x) := \#\{ n \in \mathbb{N} : n \leq x, f(n) \text{ k-free} \}
\]

Here the constant \( C(f,k) \) is given as

\[
C(f,k) := \prod_p (1 - \rho_f(p^k)p^{-k})
\]

where

\[
\rho_f(d) := \#\{ n \mod d : d \mid f(n) \}
\]

Further progress was made twenty years later by Erdős [2] who showed that one could obtain \( k \)-free values for \( k = d - 1 \), as soon as \( d \geq 3 \). For such \( k \) the asymptotic formula (1) was later obtained by Hooley [8].

The next development was due to Nair [9] who established (1) for \( k \geq (\sqrt{2} - \frac{1}{2})d \). In particular Nair’s result shows that \( k = d - 2 \) is admissible for \( d \geq 24 \). The author [4, Theorem 16] then showed how the “determinant method” could be applied to the problem, and demonstrated that the asymptotic formula remained valid for \( k \geq (3d + 2)/4 \), so that one may take \( k = d - 2 \) providing only that \( d \geq 10 \). Indeed using methods of Salberger (to appear) one can replace these inequalities by \( k \geq (3d + 1)/4 \) and \( d \geq 9 \) respectively.
In this paper we show that further progress is possible for irreducible polynomials of the form $f(X) = X^d + c$. For these we establish the following result.

**Theorem 1** Let $f(X) = X^d + c \in \mathbb{Z}[X]$ be an irreducible polynomial, and suppose that $k \geq (5d + 3)/9$. Then there is a constant $\delta(d)$ such that

$$N_{f,k}(x) = C(f, k)x + O(x^{1-\delta(d)}).$$

The implied constant may depend on $f$ and $k$.

For comparison with the earlier results we point out that this will allow $k = d - 2$ as soon as $d \geq 6$. The result of Erdős handles the case of cubic polynomials taking square-free values, and the most interesting open question then concerns quartic polynomials taking square-free values. We would therefore like to handle $k = d - 2$ for $d = 4$, and one can track our progress towards this goal through the historical discussion above.

There is a related question concerning powerfree values of $f$ at prime arguments. Here there is a natural condition that for every prime $p$ there should be an integer $n_p$, coprime to $p$, and such that $p^k \nmid f(n_p)$. With this in mind one defines

$$N'_{f,k}(x) := \# \{ p \text{ prime} : p \leq x, f(p) \text{ k-free} \}$$

and

$$C'(f, k) := \prod_p (1 - \rho'_f(p^k)\phi(p^k)^{-1})$$

where

$$\rho'_f(d) := \# \{ n \text{ mod } d : \gcd(n, d) = 1, d \mid f(n) \}. $$

The corresponding asymptotic formula

$$N'_{f,k}(x) \sim C'(f, k)\pi(x) \quad (x \to \infty)$$

has been proved for $k = d$ by Uchiyama [11], by a method that also handles the case $k > d$. However it remains an open problem to establish this in the case $k = d - 1$ considered for the previous problem by Erdős and Hooley. None the less, important progress has been made by Helfgott [6] and [7], showing in particular that the asymptotic formula holds in the case $k = 2$ and $d = 3$.

Our methods are sufficiently robust that they apply immediately to powerfree values of $f(p)$. We have the following result.
Theorem 2 Let $f(X) = X^d + c \in \mathbb{Z}[X]$ be an irreducible polynomial, and suppose that $k \geq \frac{5d + 3}{9}$. Suppose that for every prime $p$ there is an integer $n_p$, coprime to $p$, and such that $p^k \nmid f(n_p)$. Then for any fixed $A > 0$ we have

$$N'_{f,k}(x) = C'(f,k)\pi(x) + O_A(x(\log x)^{-A}).$$

In particular this holds for $k = d - 1$ and every $d \geq 3$.

The preliminary manoeuvres for these problems are straightforward. We shall fix the polynomial $f$ (and hence also $d$) throughout, so that all order constants may depend tacitly on $f$ and $d$. The key fact we shall use is that

$$\sum_{b^k \mid f(n)} \mu(b) = \begin{cases} 1, & f(n) \text{ is } k\text{-free,} \\ 0, & \text{otherwise.} \end{cases}$$

It follows that

$$N_{f,k}(x) = \sum_b \mu(b)N(b, x)$$

with

$$N(b, x) = \#\{n \leq x : b^k \mid f(n)\},$$

and similarly that

$$N'_{f,k}(x) = \sum_b \mu(b)N'(b, x)$$

with

$$N'(b, x) = \#\{p \leq x : b^k \mid f(p)\}.$$ 

Clearly $N'(b, x) = N(b, x) = 0$ for $b \gg x^{d/k}$. If we denote the solutions to $f(n) \equiv 0 \mod b^k$ by $n_1, \ldots, n_r$, where $r = \rho_f(b^k)$, then

$$N(b, x) = \sum_{i \leq r} \#\{n \leq x : n \equiv n_i \mod b^k\}$$

$$= \sum_{i \leq r} (xb^{-k} + O(1))$$

$$= x b^{-k} \rho_f(b^k) + O(\rho_f(b^k)),$$

and similarly, providing that $b \leq (\log x)^{2A}$ we have

$$N'(b, x) = \sum_{i \leq r} \#\{p \leq x : p \equiv n_i \mod b^k\}$$

$$= \sum_{i \leq r, (n_i, b) = 1} \pi(x; b^k, n_i)$$

$$= \frac{\pi(x)}{\phi(b^k)} \rho_f'(b^k) + O_A(\rho_f(b^k)x(\log x)^{-4A}),$$

where $\rho_f$ is the irrationality measure of any root of $f$. If $f$ is of degree 3 we may take $\rho_f \approx 2.4$, and if $f$ is of degree 4 we may take $\rho_f \approx 2.5$. It follows that

$$\rho_f = \frac{1}{2} \log 2 + O_{f,k}(x(\log x)^{-\epsilon})$$

for any $\epsilon > 0$.
by the Siegel-Walfisz Theorem. Now, for any $\xi > 0$ we find that

$$\sum_{b \leq \xi} \mu(b)N(b, x) = x \sum_{b \leq \xi} \frac{\mu(b)\rho_f(b^k)}{b^k} + O(\sum_{b \leq \xi} \rho_f(b^k)).$$

The function $\rho_f$ is multiplicative, with $\rho(p^k) \ll 1$, whence

$$\rho(b^k) \ll \varepsilon b^\varepsilon$$

for any $\varepsilon > 0$ and any square-free $b$. If $k \geq 2$ it follows on taking $\varepsilon = 1/2$ that

$$\sum_{b \leq \xi} \frac{\mu(b)\rho_f(b^k)}{b^k} = \sum_{b=1}^\infty \frac{\mu(b)\rho_f(b^k)}{b^k} + O(\sum_{b > \xi} b^{1/2-k}) = C(f, k) + O(\xi^{-1/2})$$

and

$$\sum_{b \leq \xi} \rho_f(b^k) \ll \xi^{3/2}.$$

In particular if we set $\xi = x^{1/2}$ we see that

$$\sum_{b \leq \xi} \mu(b)N(b, x) = C(f, k)x + O(x^{3/4}).$$

In precisely the same way, if we take $\xi = (\log x)^{2A}$, then

$$\sum_{b \leq \xi} \mu(b)N'(b, x) = C'(f, k)\pi(x) + O_A(x(\log x)^{-A}).$$

We now consider the range $\xi < b \leq x^{1-\eta}$, where $\eta$ is a small positive constant. Here we have

$$\sum_{\xi < b \leq x^{1-\eta}} \mu(b)N(b, x) \ll \sum_{\xi < b \leq x^{1-\eta}} N(b, x) \ll \sum_{\xi < b \leq x^{1-\eta}} \left(\frac{x}{b^k} + O(1)\right) \rho_f(b^k).$$

If we use the bound (2) with $\varepsilon = \frac{1}{2}\eta \leq \frac{1}{2}$ this yields

$$\sum_{\xi < b \leq x^{1-\eta}} \mu(b)N(b, x) \ll x^{\xi^{-1/2}} + x^{1-\eta/2} \ll x^{1-\eta/2}.$$
To complete the proof of the two theorems it will now be enough to show that

\[ \sum_{x^{1-\eta} < b \leq x^{d/k}} N(b, x) \ll x^{1-\delta} \]

for some \( \delta > 0 \), providing that \( \eta \) is small enough. By a suitable dyadic subdivision we then see that it will suffice to establish the following estimate.

**Lemma 1** Let \( f(X) = X^d + c \in \mathbb{Z}[X] \) be an irreducible polynomial. For any \( N, A, B \in \mathbb{N} \) define

\[
F(N; A, B) := \# \{ (n, a, b) \in \mathbb{N}^3 : f(n) = ab^k, N < n \leq 2N, A < a \leq 2A, B < b \leq 2B \}.
\]

Then if \( (5d + 3)/9 \leq k \leq d - 1 \) there is a constant \( \delta \) depending on \( d \) such that

\[ F(N; A, B) \ll_f N^{1-\delta} \]

for \( B \geq N^{1-\delta} \).

We have now reduced our problem to one of counting solutions to a Diophantine equation \( f(n) = ab^k \), inside a suitable box. A general procedure for such questions is provided by the “determinant method” developed in the author’s paper [3]. The efficiency of the method depends on the dimension of the associated algebraic variety. For \( f(n) = ab^k \) we are counting integer points on an affine surface. Thus far we have made no use of the special shape of the polynomial \( f \), but if we observe that \( f(n) = n^d + O(1) \) we see that \( (n, a, b) \) lies close to the weighted projective curve \( X_0^d = X_1^k X_2^k \), where \( X_0 \) and \( X_2 \) are given weight 1, and \( X_1 \) has weight \( d - k \). Thus the particular form of the polynomial \( f \) allows us to consider points close to a curve, rather than points on a surface. Reducing the dimension in this way is the key to our saving. The procedure is discussed in more detail in the author’s work [5], to which the interested reader should be directed.

## 2 The Determinant Method

Since \( f(n) = n^d + O(1) \) we will have

\[ N^d B^{-k} \ll A \ll N^d B^{-k} \tag{3} \]

for large \( N \). Moreover, since \( a \geq 1 \) we may assume that \( B^k \ll N^d \), and indeed we shall assume that

\[ N^{1-\eta} \ll B \ll N^{d/k} \tag{4} \]
for some positive constant $\eta$. We will choose a parameter $K \geq 1$ having
\[
1 \ll \frac{\log K}{\log N} \ll 1,
\] (5)
and divide the available range for $n/b$ into $O(K)$ subintervals
\[
I = (m_0N/BK, (m_0 + 1)N/BK]
\] with endpoints defined by integers $m_0$ in the range
\[
K \ll m_0 \ll K.
\] (6)
We use $F_I(N; A, B)$ to denote the corresponding contribution to $F(N; A, B)$. Since $f(n) = n^d + O(1)$ we have $n^d = ab^k + O(1)$ and
\[
(n/b)^d = a/b^{d-k} + O(B^{-d}).
\]
It will be convenient to put $k = d - j$ so that
\[
(n/b)^d = a/b^j + O(B^{-d}).
\] (7)
We now begin the determinant method by listing the points $(n_r, a_r, b_r)$ contributing to $F_I(N; A, B)$. Thus the index $r$ runs from 1 to
\[
R := F_I(N; A, B).
\]
We choose an integer parameter $D \geq 1$ and consider the monomials
\[
m(n, a, b) = n^u a^v b^w
\] for which $u + jv + w = D$. Thus we may consider $D$ as the weighted degree of the monomial, where the variables $(n, a, b)$ are given weights $(1, j, 1)$. The number of such monomials will be
\[
H := \sum_{v \leq D/j} (D - jv + 1) = \frac{D^2}{2j} + O(D)
\] (8)
and we label them as $m_1(n, a, b), \ldots, m_H(n, a, b)$. We now proceed to consider the $R \times H$ matrix $M$ say, whose $(r, h)$ entry is $m_h(n_r, a_r, b_r)$. The strategy of the determinant method is to show that $M$ has rank strictly less than $H$, if the parameters $K$ and $D$ are suitably chosen. If this can be achieved, there will be a non-zero integer vector $\bar{c}$ such that $M\bar{c} = 0$. This vector will
depend on the interval \( I \), that is to say it will depend on \( m_0 \). It provides the coefficients of a weighted homogeneous polynomial

\[
C_I(n, a, b) = \sum_h c_h m_h(n, a, b)
\]
such that

\[
C_I(n_r, a_r, b_r) = 0, \quad (r \leq R).
\] (9)

If \( R < H \) the matrix \( M \) automatically has rank less than \( H \). Otherwise it suffices to show that any \( H \times H \) sub-determinant vanishes, and it will be enough to consider the determinant formed from the first \( H \) rows of \( M \), which we shall denote by \( \Delta \). Clearly \( \Delta \) is an integer, and our strategy is to show that \( |\Delta| < 1 \) so that \( \Delta \) must vanish.

We proceed to divide the \( r \)-th row of \( \Delta \) by \( b_r^D B^{-D} \) for each \( r \leq D \), and similarly to divide the column corresponding to the monomial \( n^u a^v b^w \) by \( N^u A^v B^w \). Since

\[
n^u a^v b^w = \left( \frac{b}{B} \right)^D \left( \frac{nB}{bN} \right)^u \left( \frac{aB^j}{b^j A} \right)^v N^u A^v B^w
\]

for \( u + jv + w = D \), this produces a new determinant \( \Delta_1 \) whose entries are of the form \( m_h(nB/bN, aB^j/b^j A, 1) \). Moreover we have

\[
|\Delta| = |\Delta_1| \prod_{r \leq H} \left( \frac{b_r}{B} \right)^D \prod_{u,v,w} N^u A^v B^w \leq 2^{HD} P |\Delta_1|,
\] (10)

where

\[
P = \prod_{u+jv+w=D} N^u A^v B^w.
\]

If we write \( B = N^\beta \) then we have \( \log A = (d - k\beta) \log N + O(1) \), by (3). It follows that

\[
\log P = (\log N) \sum_{u+jv+w=D} (u + v(d - k\beta) + w\beta) + O_D(1)
\]

\[
= (\log N) \left\{ \frac{D^3}{6j} (1 + (d - k\beta)j^{-1} + \beta) + O(D^2) \right\} + O_D(1). \quad (11)
\]

We now write

\[
\frac{n_r B}{b_r N} = \frac{m_0}{K} + s_r, \quad \text{and} \quad \frac{a_r B^j}{b_r^j A} = \frac{N^d}{AB^x} \left( \frac{m_0}{K} + s_r \right)^d + t_r.
\]

Since \( n_r/b_r \in (m_0 N/BK, (m_0 + 1)N/BK) \) it follows that

\[ s_r \ll K^{-1}. \]
Moreover (3) and (7) yield
\[ \frac{a_r B^j}{b_r A} = \frac{N^d}{AB^k} \left( \frac{n_r B}{b_r N} \right)^d + O(N^{-d}), \]
and hence
\[ t_r \ll N^{-d}. \]
Thus the \((r, h)\) entry of \(\Delta_1\) will be a polynomial
\[ f_h(s_r, t_r) = (m_0 K^{-1} + s_r)^n \left( N^d A^{-1} B^{-k} (m_0 K^{-1} + s_r)^d + t_r \right)^v. \]
Clearly \(f_h\) may depend on \(h, m_0, K, D\) and \(d\), but it is independent of \(r\).
Moreover the degree of \(f_h\) will be at most \(dD\). It follows from (3) and (6) that \(N^d A^{-1} B^{-k} \ll 1\) and \(m_0 K^{-1} \ll 1\), whence we have the bound \(||f_h|| \ll D^{-1}\) for the height of \(f_h\).

In order to estimate the size of \(\Delta_1\) we will use Lemma 3 of the author’s work [5]. For each of the monomials \(s^u t^v\) we write
\[ \|s^u t^v\| = K^{-u} N^{-dc}, \]
and we list them in order as \(m_1, \ldots, m_H\) with \(\|m_1\| \geq \|m_2\| \geq \ldots\). Then according to [5, Lemma 3] we have
\[ \Delta_1 \ll D \left( \max_{h=1}^H \|f_h\| \right)^H \prod_{h=1}^H \|m_h\| \ll D \prod_{h=1}^H \|m_h\|. \tag{12} \]
To proceed further we shall write \(K = N^{\kappa}\), and note that \(1 \ll \kappa \ll 1\), by [5]. If we now write \(m(\lambda)\), say, for the number of monomials \(m_r = s^u t^v\) with \(\|m_r\| \geq N^{-\lambda}\), then
\[ m(\lambda) = \# \{(u, v) \in \mathbb{Z}^2 : u, v \geq 0, \kappa u + dv \leq \lambda\} = \frac{\lambda^2}{2kd} + O(\lambda) + O(1). \]
If \(\|m_H\| = N^{-\lambda_0}\) then \(m(\lambda_0) \geq H\), while for any \(\varepsilon > 0\) we will have
\[ m(\lambda_0 - \varepsilon) \leq H - 1. \]
We may therefore deduce that
\[ \lambda_0 = \sqrt{2kdH} + O(1). \]
We then find that
\[ \prod_{h=1}^H \|m_h\| = N^{-\mu}. \]
with
\[
\mu = \sum_{\kappa u + dv \leq \lambda_0} (\kappa u + dv) + O(\lambda_0^2) + O(1) \\
= \frac{\lambda_0^3}{3kd} + O(\lambda_0^2) + O(1) \\
= \frac{2^{3/2}}{3} (kd)^{1/2} H^{3/2} + O(H).
\]

In view of (8), (10), (11) and (12) we may now conclude that
\[
\log |\Delta|/\log N \leq \frac{D^3}{6j} (1 + (d-k\beta)j^{-1} + \beta) - \frac{2^{3/2}}{3} (kd)^{1/2} H^{3/2} + O_D((\log N)^{-1}) + O(D^2).
\]

Thus (8) yields
\[
\frac{\log |\Delta|}{D^3 \log N} \leq \frac{1}{6j} (1 + (d-k\beta)j^{-1} + \beta) - \frac{2^{3/2}}{3} (kd)^{1/2} (2j)^{-3/2} \\
+ O_D((\log N)^{-1}) + O(D^{-1}).
\]

We therefore choose
\[
\kappa = \frac{j}{4d} \left( 1 + \frac{d-k\beta}{j} + \beta \right)^2 + \eta,
\]
with the same small constant \(\eta\) as in (11). Then (5) will be satisfied, and we will have
\[
\frac{\log |\Delta|}{D^3 \log N} < 0
\]
providing that we first choose \(D = D(f,d,\eta)\) sufficiently large, and then ensure that \(N\) is sufficiently large in terms of \(f, d\) and \(\eta\).

We therefore deduce that \(\Delta = 0\) when \(K = N^\kappa\). With this choice the matrix \(M\) introduced at the beginning of the section will have rank strictly less than \(H\), so that all solutions \((n_r, a_r, b_r)\) counted by \(F_I(N; A, B)\) satisfy the auxiliary equation (9).

### 3 Completion of the Proof

We now complete our estimation of \(F_I(N; A, B)\) by considering how many triples \((n,a,b)\) can satisfy both the original equation \(f(n) = ab^k\) and the additional equation (9). The procedure here will follow precisely that used in the author’s paper [4, §5.3]. Since \(C_I\) is homogeneous with exponent weights
(1, j, 1) any factor would have to be similarly weighted-homogeneous. It follows in particular that \( C_I(x, y, z) \) cannot have a factor in common with \( f(x) - yz^k \). As in [4, pages 84 and 85] we find that either

\[
F_I(N, A, B) \ll \varepsilon (1 + N/B) N^\varepsilon
\]

or that there is an irreducible polynomial \( G_I(X, Y) \in \mathbb{Z}[X, Y] \), with degree bounded in terms of \( d \) and \( \varepsilon \), but at least \( d \), such that

\[
G_I(n, b) = 0
\]

for every triple \((n, a, b)\) counted by \( F_I(N, A, B) \).

For a given interval \( I \) we will have

\[
\frac{n}{b} \in I = (m_0 N/BK, (m_0 + 1) N/BK]
\]

It therefore follows that

\[
\left| \frac{n - m_0 N}{BK} b \right| \leq \frac{2N}{K}, \quad B < b \leq 2B.
\]

It will be convenient to define a linear mapping \( T : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \) by

\[
Tx := \begin{pmatrix} K(2N)^{-1}x_1 - (2B)^{-1}m_0 x_2 \\ (2B)^{-1}x_2 \end{pmatrix}
\]

and to consider the lattice

\[
\Lambda = \{ Tx : x \in \mathbb{Z}^2 \}
\]

of determinant \( K(4NB)^{-1} \). Then if \( x = (n, b) \) satisfies (16) we produce a point \( Tn = (\alpha_1, \alpha_2) \in \Lambda \) falling in the square

\[
S = \{ (\alpha_1, \alpha_2) : \max(|\alpha_1|, |\alpha_2|) \leq 1 \}.
\]

Let \( g^{(1)} \) be the shortest non-zero vector in the lattice and \( g^{(2)} \) the shortest vector not parallel to \( g^{(1)} \). These vectors will form a basis for \( \Lambda \). Moreover we have \( \lambda_1 g^{(1)} + \lambda_2 g^{(2)} \in S \) only when \( |\lambda_1| \ll |g^{(1)}|^{-1} \) and \( |\lambda_2| \ll |g^{(2)}|^{-1} \). These constraints may be written in the form \( |\lambda_i| \leq L_i \), for appropriate bounds \( L_1, L_2 \). Since \( |g^{(2)}| \geq |g^{(1)}| \) and \( |g^{(1)}|, |g^{(2)}| \ll \det(\Lambda) \ll K(4NB)^{-1} \) we will have \( L_1 \gg L_2 \) and \( L_1 L_2 \gg NBK^{-1} \). We now write \( h^{(i)} = T^{-1} g^{(i)} \) for \( i = 1, 2 \). These vectors will then be a basis for \( \mathbb{Z}^2 \), and if \( x = \lambda_1 h^{(1)} + \lambda_2 h^{(2)} \) is in the region (16) then we will have \( |\lambda_i| \leq L_i \) for \( i = 1, 2 \). This allows us to make a
change of basis, replacing \((x_1, x_2)\) by \((\lambda_1, \lambda_2)\) so that our constraints on \(n, b\) are replaced by the conditions \(|\lambda_i| \leq L_i\).

We therefore proceed to substitute \(\lambda_1, \lambda_2\) for \(n, b\) in (15). We may then use the bound of Bombieri and Pila [1, Theorem 5] to show that the number of possible pairs \(\lambda_1, \lambda_2\) is \(\ll \varepsilon \max(L_1, L_2)^{1/d + \varepsilon} \ll \varepsilon L_1^{1/d + \varepsilon}\), since the degree of \(G\) is at least \(d\). Thus

\[
F_1(N, A, B) \ll \varepsilon L_1^{1/d + \varepsilon}.
\]

The number \(L_1\) depends on the interval \(I\), which is determined by \(m_0\). We therefore write \(L_1 = L_1(m_0)\) accordingly. In view of the alternative (14) we then see that

\[
F(N, A, B) \ll \varepsilon K \left(1 + N/B\right) N^\varepsilon + \sum_{K \ll m_0 \ll K} L_1(m_0)^{1/d + \varepsilon},
\]

(17)

the range for \(m_0\) being given by (16).

We proceed to investigate the number of choices for \(m_0\) which produce a value \(L_1(m_0)\) lying in a given dyadic interval \((L, 2L]\) say. In the notation above, if \((n, b) = (x_1, x_2)\) corresponds to \(g^{(1)}\) then

\[
L_1 \left(x_1 - \frac{m_0 N}{BK} x_2\right) \ll \frac{N}{K}
\]

and \(L_1 x_2 \ll B\). Moreover we will have \(\gcd(x_1, x_2) = 1\). Thus the number of intervals \(I\) for which \(L < L_1 \leq 2L\) is at most the number of triples \((x_1, x_2, m_0) \in \mathbb{Z}^3\) with \(\gcd(x_1, x_2) = 1\), for which

\[
L \left(x_1 - \frac{m_0 N}{BK} x_2\right) \ll \frac{N}{K}, \quad L x_2 \ll B, \quad \text{and} \quad K \ll m_0 \ll K.
\]

(18)

We proceed to consider whether the value \(x_2 = 0\) can occur. If \(x_2 = 0\) the first of the conditions above would yield \(L x_1 \ll N/K\). However we cannot have \(x_1 = x_2 = 0\), so that we must have \(L \ll N/K\) whenever \(x_2 = 0\). We now recall that \(L_1 \gg L_2\) and that \(L_1 L_2 \gg NBK^{-1}\), whence

\[
L^2 \gg NBK^{-1}.
\]

(19)

It follows that if \(x_2 = 0\) then \((N/K)^2 \gg L^2 \gg NBK^{-1}\) and hence that \(BK \ll N\). However, since \(K = N^\kappa\) with \(\kappa\) given by (13), we see from (4) that \(BK/N\) tends to infinity with \(N\), which ensures that the case \(x_2 = 0\) cannot arise.

We now see in particular that the second condition of (18) yields \(L \ll B\). If we rewrite the first of the conditions (18) to say that

\[
m_0 x_2 = N^{-1} BK x_1 + O(BL^{-1})
\]
we then see that each choice for $x_1$ restricts the product $m_0x_2$ to an interval of length $\ll B/L$, with $B/L \gg 1$. Moreover $m_0x_2$ is never zero. Thus a divisor function estimate shows that there are $O_\varepsilon(N^\varepsilon BL^{-1})$ possible pairs $(x_2, m_0)$ for each value of $x_1$. The conditions (18) show that $x_1 \ll N/L$, so that $x_1$ takes $O(1+N/L)$ values. This allows us to conclude that the number of integers for $m_0$ which produce a value $L_1(m_0)$ in the range $L < L_1 \leq 2L$ is $O_\varepsilon((1+N/L)N^\varepsilon BL^{-1})$.

We can now feed this information into (17), using a dyadic subdivision for the values of $L_1(m_0)$ to obtain

$$F(N, A, B) \ll \varepsilon K(1+N/B)N^\varepsilon + \sum_L L^{1/d+\varepsilon}(1+N/L)N^\varepsilon BL^{-1},$$

in which $L$ runs over powers of 2, subject to the condition $L \gg (NBK^{-1})^{1/2}$ given by (19). It then follows that

$$F(N, A, B) \ll \varepsilon K(1+N/B)N^\varepsilon + L_0^{1/d+\varepsilon}(1+N/L_0)N^\varepsilon BL_0^{-1},$$

where $L_0 := \max\{1, (NBK^{-1})^{1/2}\}$. On taking $\varepsilon = \eta$ we deduce from (4) that

$$F(N, A, B) \ll \eta N^{2\eta}\{K + L_0^{1/d+\eta}(1+N/L_0)BL_0^{-1}\}.$$

We proceed to analyse our estimate for $F(N, A, B)$ by defining

$$\rho(t) = \frac{j}{4d} \left(1 + \frac{d - kt}{j} + t\right)^2$$

and $q(t) = \rho(t) + 1 - t$. Then

$$q'(t) = \frac{j}{d} \left(1 + \frac{d - kt}{j} + t\right) \left(1 - \frac{k}{j}\right) - 1.$$

This is clearly negative if $k \geq j$ and $0 \leq t \leq d/k$. Hence if $k \geq d/2$ we have

$$q(t) \geq q(d/k) = \frac{j^3}{4dk^2} \geq 0$$

for $0 \leq t \leq d/k$. It therefore follows that $KN \leq B$, and hence that $L_0 \leq N$ for the relevant range of $B$. Our estimate now simplifies to give

$$F(N, A, B) \ll \eta N^{2\eta}\{K + L_0^{-2+1/d+\eta}NB\}.$$

This will be of order $N^{1-\eta}$ if $\eta > 0$ is sufficiently small, and

$$\sup_{1 \leq t \leq d/k} \rho(t) < 1 \quad \text{and} \quad \sup_{1 \leq t \leq d/k} Q(t) < 0$$

12
for

\[ Q(t) = \left( -2 + \frac{1}{d} \right) \frac{1 + t - k(t)}{2} + t. \]

To handle the condition on \( \rho(t) \) we note that the function attains its supremum at either \( t = 1 \) or \( t = d/k \). Moreover if \( v = k/d \) satisfies \( 5/9 < v < 1 \) we find that \( \rho(1) = 9(1 - v)/4 < 1 \) and

\[ \rho(d/k) = \frac{(1 + v)(1 - v^2)}{4v^2}. \]

This latter function is decreasing with respect to \( v \), and takes the value \( 196/225 < 1 \) at \( v = 5/9 \). It follows that the supremum is strictly less that 1 if \( 5/9 < k/d < 1 \).

To verify the condition on \( Q(t) \) we note that if \( 1 \leq t \leq d/k \) then

\[
Q'(t) = \left( -2 + \frac{1}{d} \right) \frac{1}{2} \left\{ 1 - \frac{j}{2d} \left( 1 + \frac{d - kt}{j} + t \right) \left( -\frac{k}{j} + 1 \right) \right\} + 1 \\
= \frac{1}{2d} - \left( 1 - \frac{1}{2d} \right) \frac{2k - d}{2d} \left( 1 + \frac{d - kt}{j} + t \right) \\
\leq \frac{1}{2d} - \left( 1 - \frac{1}{2d} \right) \frac{2k - d}{2d} \left( 1 + \frac{d}{k} \right) \\
< 0
\]

for \( k > d/2 \). Thus

\[ Q(t) \leq Q(1) = \frac{9j}{4d} \left( 1 - \frac{1}{2d} \right) - \left( 1 - \frac{1}{d} \right), \]

which is strictly negative for

\[ j < \frac{4d^2}{9d - 2}. \]

This condition is equivalent to

\[ k > \frac{10d^2 - d}{18d - 9} = \frac{5d + 2}{9} + \frac{2}{18d - 9}. \]

Thus it is necessary and sufficient that

\[ k \geq \frac{5d + 3}{9}. \]

This completes the proof of Lemma \( \square \) and hence also of our two theorems.
References

[1] E. Bombieri and J. Pila, The number of integral points on arcs and ovals, *Duke Math. J.*, 59 (1989), 337-357.

[2] P. Erdős, Arithmetical properties of polynomials, *J. Lond. Math. Soc.*, 28 (1953), 416–425.

[3] D.R. Heath-Brown, The density of rational points on curves and surfaces, *Ann. of Math. (2)*, 155 (2002), 553–595.

[4] D.R. Heath-Brown, Counting rational points on algebraic varieties, *Analytic number theory*, 51–95, Lecture Notes in Math., 1891, Springer, Berlin, 2006.

[5] D.R. Heath-Brown, Sums and differences of three $k$th powers, *J. Number Theory*, 129 (2009), 1579-1594.

[6] H.A. Helfgott, Power-free values, large deviations and integer points on irrational curves, *J. Théor. Nombres Bordeaux*, 19 (2007), no. 2, 433–472.

[7] H.A. Helfgott, Power-free values, repulsion between points, differing beliefs and the existence of error, *Anatomy of integers*, 81–88, CRM Proc. Lecture Notes, 46, (Amer. Math. Soc., Providence, RI, 2008).

[8] C. Hooley, On the power free values of polynomials, *Mathematika*, 14 (1967), 21–26.

[9] M. Nair, Power free values of polynomials, *Mathematika*, 23 (1976), 159–183.

[10] G. Ricci, Ricerche aritmetiche sui polinomi, *Rend. Circ. Mat. Palermo*, 57 (1933), 433–475.

[11] S. Uchiyama, On the power-free values of a polynomial, *Tensor (N.S.*), 24 (1972), 43–48.

Mathematical Institute,
24–29, St. Giles’,
Oxford
OX1 3LB
UK

rhb@maths.ox.ac.uk