POWERFREE VALUES OF BINARY FORMS

Michael Filaseta*

1. Introduction

Given a binary form $f(x,y) \in \mathbb{Z}[x,y]$, we will be interested in finding the smallest k for which we can establish that there are infinitely many integers a and b such that $f(a,b)$ is $k-$free. Necessarily, we require the f has no fixed kth prime power divisor. Until the final section of this paper, we will also consider f to be irreducible. We set $n = \deg f$. For $k = 2$, this problem has recently become of interest partially because of its connection to the rank of elliptic curves as described in the work of F. Gouvêa and B. Mazur [4]. In particular, F. Gouvêa and B. Mazur showed that if the degree of the binary form is ≤ 3, then $f(a,b)$ is squarefree for infinitely many pairs of integers a and b. More specifically, for a binary form $f(x,y) \in \mathbb{Z}[x,y]$ of degree ≤ 3, they determined the density of pairs (a,b) of positive integers for which $f(a,b)$ is squarefree, i.e., the value of

$$\lim_{X\to\infty} \frac{|\{(a,b) \in (\mathbb{Z}\cap[1,X])^2 : f(a,b) \text{ squarefree}\}|}{X^2}.$$

This result was extended by G. Greaves [6] to binary forms of degree ≤ 6. The main tool for these results was a technique of Hooley [8] which dealt with the corresponding problem for single variable polynomials. For $f(x) \in \mathbb{Z}[x]$ of degree ≤ 3, Hooley's method gives the asymptotic density for the number of integers m such that $f(m)$ is squarefree. For $f(x) \in \mathbb{Z}[x]$ of degree n and general k, Hooley obtained the asymptotic density for the number of integers m such that $f(m)$ is $k-$free whenever $k \ge n-1$. For binary forms,

*Research was supported in part by the NSA under grant number MDA904-92-H-3011

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

G. Greaves [6] obtained the density for the number of pairs (a, b) for which $f(a, b)$ is $k-$free whenever $k \geq [n/2]$. Observe that the previously mentioned result of G. Greaves for $k = 2$ is slightly stronger than the result obtained by replacing k with 2 in the more general result.

There is a reasonable next step to consider based on the development of the single variable problem after Hooley's work in [8]. M. Nair [10,11] and M. Huxley and M. Nair [9] showed some improvements can be made in the single variable case. In particular, if the degree of $f(x)$ is $\leq n$, then Hooley's approach gives the asymptotic density described above whenever $k \geq n-1$ whereas the approach of Nair in [10] gives the asymptotic density whenever $k \geq \left(\sqrt{2} - \frac{1}{2}\right) n$. Since $\sqrt{2}-(1/2) < 1$, Nair's approach gives improvements when the degree is sufficiently large. More precise analysis shows that Nair's approach improves on the work of Hooley whenever $n \geq 18$ and that the modifications in Huxley and Nair [9] lead to improvements whenever $n \geq 14$. Nevertheless, Nair's approach has not led to results as strong as Hooley's when $k = 2$, and we note that the case $k = 2$ for binary forms was the main problem dealt with in Greaves [6] and is what has led to the applications to the rank of elliptic curves.

The purpose of this paper is to describe Nair's approach for the binary form problem and to improve on the work of Greaves when k is sufficiently large. In particular, we will show

Theorem. *Let k and n be positive integers with $k \geq 2$. Let $f(x, y) \in \mathbb{Z}[x, y]$ be an irreducible binary form of degree n with no fixed kth power divisor. If $k \geq (2\sqrt{2} - 1)n/4$, then a positive proportion of pairs (a, b) of integers are such that $f(a, b)$ is $k-$free.*

We observe that the constant being multiplied by n in the inequality involving k and n in the theorem is exactly one-half of the constant $\sqrt{2} - (1/2)$ appearing in Nair's result about $k-$free values of irreducible polynomials. This is somewhat expected as Hooley obtained $k \geq n - 1$ in the single variable problem and Greaves obtained the analogous result with $k \geq [n/2]$ in the binary form problem. The argument for the theorem mainly requires rewriting the argument of Nair for the single variable problem so that it applies to the binary form problem and making use of an estimate of Greaves [5,6]. We will give most of the details here to provide the reader with the author's slightly different perspectives on Nair's approach. The constant $(2\sqrt{2}-1)/4$ appearing in the theorem is the best constant the author has obtained from these methods, but (analogous to Nair's results and the work of Huxley and Nair) one can find smaller k for specific values of n. In the final section of this paper, we will briefly address this issue. In particular, we note that Greaves [6] comments that he is unable to show that for $k \geq 3$ and $n \leq 2k+2$, there are infinitely many pairs of integers (a,b) for which $f(a,b)$ is $k-$free. We will show how one can obtain such a result for $k \geq 5$. Analogous to the previous work on this problem, we will also discuss what can be said in the case that $f(x,y)$ is reducible.

2. Preliminaries

The notation we will use is as follows:

f is an irreducible binary form in $\mathbb{Z}[x,y]$ with no fixed kth prime power divisor. The degree of f is n with $n \geq 2$. Observe that in the binary form case, we get that the coefficient of x^n and the coefficient of y^n are non-zero (otherwise, f would be divisible by x or y and, hence, be reducible).

d is the leading coefficient of $f(x,1)$; in other words, d is the coefficient of x^n in $f(x,y)$.

k, a, and b will denote positive rational integers with $k \geq 2$, and we assume that f has no fixed kth power divisors.

$p, p_1, p_2, \ldots$ denote primes.

X is a sufficiently large real number, $X \geq X_0(f,k)$.

γ is a fixed root of $f(x,1)$. The identity $f(x,y) = y^n f(x/y,1)$ implies that $f(x,1)$ is irreducible in $\mathbb{Z}[x]$. Also, observe that the degree of $f(x,1)$ is n.

$K = \mathbb{Q}(\gamma)$.

R is the ring of integers in K.

$\{\omega_1, \dots, \omega_n\}$ is a fixed integral basis for K over $\mathbb{Q}$.

$\sigma_1, \dots, \sigma_n$ denote the homomorphisms of K which fix the elements of $\mathbb{Q}$.

E_j and E will denote constants in R.

$N(u) = N_{K/\mathbb{Q}}(u) = \prod_{j=1}^{n} \sigma_j(u)$ (where $u \in K$). We will also use $N(D)$ in referring to the norm of an ideal D in R.

$||u||$ denotes the size of an element u in K ($||u|| = \max_{1 \le j \le n} |\sigma_j(u)|$).

$c_1, c_2 \dots$ and implied constants, unless otherwise stated, are positive constants depending on f and k.

u is *primary* means that $||u|| \le c_1 |N(u)|^{1/n}$ where c_1 is a constant (described below or see [10]). This differs slightly from Nair's use of the word "primary," but it is sufficient for obtaining our results.

"Cubes" in $\mathbb{Z}^n$ refer to cubes with edges parallel to the axes in $\mathbb{Z}^n$.

Lemma 1. *Let $T \ge X^2/\log X$. For $f \in \mathbb{Z}[x,y]$ as above, let*

$$N_k(X) = |\{(a,b) : 1 \le a, b \le X,\ f(a,b) \text{ is } k-\textit{free}\}|,$$

$$P(X) = \left|\left\{(a,b) : 1 \le a, b \le X,\ p^k | f(a,b) \text{ for some prime } p > T\right\}\right|,$$

and

$$\rho(p^k) = \left|\left\{(i,j) \in \{0,1,\dots,p^k-1\}^2 : f(i,j) \equiv 0 \pmod{p^k}\right\}\right|.$$

Then

$$N_k(X) = X^2 \prod_p \left(1 - \frac{\rho(p^k)}{p^{2k}}\right) + O\left(\frac{X\sqrt{T}}{\sqrt{\log X}}\right) + O\left(P(X)\right)$$

and

$$P(X) \ll \max \sum 1,$$

where the maximum is over all E from a fixed finite set of algebraic integers in K and the sum is over all pairs (u,v) with u and $v \in R$, u primary, $||u|| > T^{1/n}$, and $u^k v = E(a - \gamma b)$ for some rational integers a and b with $1 \le a, b \le X$.

Observe that Lemma 1 is obvious unless $\rho(p^k) \le p^{2k} - 1$ for all p. Suppose then that this inequality holds. We will want a better but fairly simple estimate on $\rho(p^k)$ noting that a more detailed analysis of the function ρ can be found in [4]. Observe that if $f(a,b) \equiv 0 \pmod{p^k}$ and $p|b$, then either p divides a or p divides d, the coefficient of x^n in $f(x,y)$. In the first case, we get at most p^{2k-2} choices for the pair (a,b) with $0 \le a, b \le p^k - 1$. We note that we could interchange the roles of a and b. In particular, if p is sufficiently large, then there are $\le p^{2k-2}$ distinct pairs (a,b) modulo p^k such that $f(a,b) \equiv 0 \pmod{p^k}$ and $p|ab$. In the second case, p is limited to the prime divisors of d and there will be only a bounded number of such primes to consider. If $f(a,b) \equiv 0 \pmod{p^k}$ and $p \nmid b$, then $b^n f(a/b,1) \equiv f(a,b) \equiv 0 \pmod{p^k}$ implies that a/b is a root of $f(x,1)$ modulo p^k. The number of such roots is $\le n$ if $p \nmid d\Delta$ where Δ is the discriminant of $f(x,1)$. Thus, for each prime p not dividing $d\Delta$ and each b relatively prime to p, we get $\le n$ choices for a modulo p^k such that $f(a,b) \equiv 0 \pmod{p^k}$. This gives $\le np^k$ values for the pair (a,b) in this case. Hence,

$$\rho(p^k) \le p^{2k-2} + np^k \ll p^{2k-2} \qquad \text{provided } p \nmid d\Delta.$$

To prove Lemma 1, we set $\xi = \epsilon \log X$, where $\epsilon > 0$ will be specified momentarily, and estimate the three quantities

$$S_1 = \left|\left\{(a,b) : 1 \le a, b \le X,\, p^k \nmid f(a,b) \text{ for every } p \le \xi\right\}\right|,$$

$$S_2 = \left|\left\{(a,b) : 1 \le a, b \le X,\, p^k | f(a,b) \text{ for some } p \in (\xi, T]\right\}\right|,$$

and

$$S_3 = \left|\left\{(a,b) : 1 \le a, b \le X,\, p^k | f(a,b) \text{ for some } p > T\right\}\right|.$$

Thus, $N_k(x) = S_1 + O(S_2) + O(S_3)$.

One can estimate S_1 with a simple sieve argument. Specifically, setting $\mathcal{P} = \prod_{p \le \xi} p$ and using the trivial estimate $\rho(p^k) \le p^{2k}$, one has that

$$S_1 = \sum_{j|\mathcal{P}} \mu(j) \prod_{p|j} \rho(p^k) \left(\frac{X}{p^k} + O(1)\right)^2 = X^2 \prod_{p \le \xi} \left(1 - \frac{\rho(p^k)}{p^{2k}}\right) + O\left(X \prod_{p \le \xi} (1 + p^{2k})\right).$$

Observe that

$$\prod_{p\le\xi}(1+p^{2k}) \le \prod_{p\le\xi}(2p^{2k}) \ll 2^{\pi(\xi)}e^{2k\xi}.$$

Taking $\epsilon = 1/(5k)$, we get that

$$S_1 = X^2 \prod_{p\le\xi}\left(1-\frac{\rho(p^k)}{p^{2k}}\right) + O\left(X^{3/2}\right).$$

Since X is sufficiently large, the primes p that divide $d\Delta$ are $\le \xi$ so that if we extend the product above to a product over all the primes and use the bound we found for $\rho(p^k)$ when $p \nmid d\Delta$, we obtain

$$S_1 = X^2 \prod_{p}\left(1-\frac{\rho(p^k)}{p^{2k}}\right) + O\left(\frac{X^2}{\log X}\right),$$

where we can conclude that the product here converges. The condition that $T \ge X^2 \log X$ in Lemma 1 implies that the error term above is $\ll X\sqrt{T}/\sqrt{\log X}$.

For an upper bound on S_2, we mainly refer to Greaves' work [5,6]. Recall the estimate $\rho(p^k) \le p^{2k-2} + np^k$ if $p \nmid d\Delta$. We may suppose that ξ is sufficiently large so that $p > \xi \implies p \nmid d\Delta$. Also, we may suppose that p does not divide the coefficient of y^n in $f(x,y)$. The terms p^{2k-2} and np^k in this bound for $\rho(p^k)$ arose from two separate considerations: (i) pairs (a,b) such that $p^k|f(a,b)$, $p|a$, and $p|b$, and (ii) other pairs (a,b). Since $1 \le a,b \le X$, we get that there are $\le ((X/p)+O(1))^2$ pairs (a,b) as in (i). In other words, we get a contribution of

$$\le \sum_{\xi<p\le T}\left(\frac{X}{p}+O(1)\right)^2 = O\left(\frac{X^2}{\log X}\right) + O(X\log\log T) + O(\pi(T))$$

pairs (a,b) as in (i). We can ignore the second error term since it is smaller than at least one of the other two error terms. The statement of Lemma 1 becomes trivial if $T \ge X^2 \log X$, and for other T as in the lemma, it is easily checked that the remaining error terms above are $\ll X\sqrt{T}/\sqrt{\log X}$.

For S_2, it remains to estimate the number of pairs (a,b) in (ii) for which $p^k|f(a,b)$ and $p \nmid ab$ for some prime $p \in (\xi, T]$. We use Lemma 2 in Greaves paper [6] which provides such an estimate. In the notation of that paper, one needs to take $\eta = T/X^2$ and note that the condition $\eta \geq (\log X)^{-2}$ that appears there should read $\eta \geq (\log X)^{-1}$. We get here that the number of pairs (a, b) in (ii) is $\ll X\sqrt{T}/\sqrt{\log X}$.

By definition $S_3 = P(X)$ so that the estimate for $N_k(X)$ in the statement of Lemma 1 follows. We are left with establishing the upper bound for $P(X)$, and we will follow Nair [10] closely here.

Fix ideals $D_1, D_2, \dots, D_h$ of R which represent the various ideal classes of K. For each D_i, there corresponds a unique D_j such that $D_i^k D_j$ is principal. For each such i and j, fix δ_i such that $D_i^k D_j = (\delta_i)$. Let $E_i = d\delta_i$. We will take the maximum in the bound for $P(X)$ in Lemma 1 to be over $E \in \{E_1, \dots, E_h\}$. To establish the bound for $P(X)$ in the lemma, it suffices to show that for each pair (a, b) of integers with $1 \leq a, b \leq X$ and with $f(a, b)$ divisible by a prime $> T$, there exists $E \in \{E_1, \dots, E_h\}$ and elements u and v of R such that u is primary, $||u|| > T^{1/n}$, and $u^k v = E(a - \gamma b)$ (where here we are using that if two different pairs (a, b) give rise to the same pair (u, v), then the corresponding values of E must be different).

Since $T > X^2/\log X$ and X is sufficiently large, we deduce that

$$p > T \implies p \nmid d\Delta.$$

Since γ is a root of $f(x, 1)$, we get that

$$d^{n-1} f(x, y) = (dx - d\gamma y) g(x, y),$$

where d, $d\gamma$, and the coefficients of $g(x, y)$ all lie in R. Also, observe that $g(x, y)$ is a form of degree $n - 1$. Let $p > T$ and (a, b) be such that $p^{k'} || f(a, b)$ for some $k' \geq k$. We get that the ideal $(p)^{k'}$ divides the ideal $(da - d\gamma b)(g(a, b))$. We factor (p) as

$$(p) = \mathcal{P}_1 \mathcal{P}_2 \cdots \mathcal{P}_r,$$

where, since $p > T$, the prime ideals $\mathcal{P}_j$ are distinct.

We show that each $\mathcal{P}_j$ divides only one of $(da - d\gamma b)$ and $(g(a, b))$. Suppose to the contrary that $\mathcal{P}_j$ divides both $(da - d\gamma b)$ and $(g(a, b))$. Then $da \equiv d\gamma b \pmod{\mathcal{P}_j}$ so that

$$0 \equiv d^{n-1} g(a, b) \equiv g(da, db) \equiv g(d\gamma b, db) \equiv b^{n-1} g(d\gamma, d) \pmod{\mathcal{P}_j}.$$

On the other hand, $p > T > X^2/\log X > b$ and $\mathcal{P}_j|(p)$ so that the above congruence implies that $\mathcal{P}_j|(g(d\gamma, d))$. Since d and γ are fixed, taking norms, we get that p divides a fixed finite number. Since $p > T$ and, hence, sufficiently large, this can only happen if $g(d\gamma, d) = 0$ or, in other words, if $g(\gamma, 1) = 0$. This is impossible as we would then get that γ is a multiple root of $f(x, 1)$ and, therefore, $f(x, y)$ is reducible. Thus, each $\mathcal{P}_j$ divides only one of $(da - d\gamma b)$ and $(g(a, b))$.

Next, we observe that the norm of the ideal $(da - d\gamma b)$ is $|d^{n-1}f(a, b)|$ which is divisible by p. It follows that some $\mathcal{P}_j$ divides $(da - d\gamma b)$. Fix such a j, and set $\mathcal{P} = \mathcal{P}_j$. Then, by the previous paragraph, there is an ideal $\mathcal{B}$ such that

$$(da - d\gamma b) = \mathcal{P}^k \mathcal{B}.$$

Recall the definition of the D_i. For some D_i and some D_j, we have that $\mathcal{P}D_i$ and $\mathcal{B}D_j$ are principal ideals in R. We use the following lemma, a proof of which can be found in [12].

Lemma 2. *Given any principal ideal in R, there exists a generator u such that $||u|| \le c_1|N(u)|^{1/n}$ (i.e., such that u is primary).*

Thus, there exist u and u' in R with u primary such that

$$D_i^k D_j (da - d\gamma b) = D_i^k \mathcal{P}^k D_j \mathcal{B} = (u)^k (u').$$

This implies that $D_i^k D_j$ is principal. From the definition of E_i, we get that

$$E_i(a - \gamma b) = u^k v$$

for some v in R. Also, observe that since $\mathcal{P}$ is a prime ideal dividing both (p) and (u) with p a rational prime, we get that $p|N(\mathcal{P})$ and $N(\mathcal{P})|N(u)$ so that $||u||^n \ge |N(u)| \ge p > T$. Hence, we get the condition $||u|| > T^{1/n}$ in the summation in Lemma 1. This completes the proof of that lemma.

Before continuing, we briefly explain the reason we have chosen to define u being primary in a slightly different manner than Nair in [10]. There the inequality in Lemma 2 was replaced by the (apparently) stronger inequality

$$c_2|N(u)|^{1/n} \le ||u|| \le c_1|N(u)|^{1/n}.$$

Nair uses this inequality to formulate the definition of u being primary. Indeed, this is how c_1 is chosen for our definition of primary (i.e., one uses Lemma 2 above to define c_1). The reason we have chosen not to also include the inequality involving c_2 in our definition is simply a matter of taste. If we ever need such an inequality, we can still use it since

$$|N(u)| \leq ||u||^n \implies ||u|| \geq |N(u)|^{1/n}.$$

Observe that, in fact, we have already made use of this inequality in the last step of the proof of Lemma 1.

We note immediately that for the purposes of the theorem, we will choose $T = X^2$ in Lemma 1 so that the error term $O(X\sqrt{T}/\sqrt{\log X})$ is smaller than the main term. This choice of T indicates a significant difference (observed by Greaves [6]) between the binary form problem and the single variable problem. The latter requires a considerably smaller choice of T. To obtain our results, we are now left with estimating $P(X)$. We observe that since there are only finitely many fixed possibilities for E_j in the maximum appearing for our upper bound on $P(X)$ in Lemma 1, we may fix $E \in R$ and write

$$\begin{aligned} P(X) \ll |\{(u,v) \in & R^2 : u \text{ primary}, ||u|| > T^{1/n}, \\ & u^k v = E(a - \gamma b) \text{ for some } (a,b) \in (\mathbb{Z} \cap [1,X])^2\}|, \end{aligned}$$

where it is understood that our bound on the right-hand side above (other than implied constants) will be independent of E. To estimate the right-hand side, we consider $H = H(X,T)$ to be determined explicitly later, and divide the interval $[1,X]$ into $[X/H]+1$ subintervals of length $\leq H$. Let I and J denote two fixed, not necessarily distinct, such subintervals. Let S denote the set of $u \in R$ such that u is primary and such that there is a $v \in R$ and rational integers $a \in I$ and $b \in J$ for which $u^k v = E(a - \gamma b)$. In a moment, we will show that if H is chosen appropriately, then each $u \in S$ is such that the corresponding v for which $u^k v = E(a - \gamma b)$ is unique. Define

$$\mathcal{S}(t) = \{u \in S : t^{1/n} < ||u|| \leq 2t^{1/n}\}.$$

Clearly, $\mathcal{S}(t)$ depends on the sets I and J, but we have suppressed this dependence to emphasize that our goal is to find an upper bound for $|\mathcal{S}(t)|$ for $t \geq T$ that is independent of I and J. For example, to establish the theorem, we will show that for any $s \in \{1, 2, \dots, k-1\}$, one has

$$|\mathcal{S}(t)| \ll X^{n/(2s+1)} t^{(s-k)/(2s+1)}.$$

We clarify, however, that such a bound will depend on a proper choice for H. Observe that if $|\mathcal{S}(t)| \ll B(X,t)$ where $B(X,t)$ is a function of X and t only, then we can conclude that

$$P(X) \ll \left(\sum_{j=0}^{\infty} B(X, 2^{jn}T) \right) \left(\frac{X}{H} + 1 \right)^2,$$

where the second factor indicates a bound on the number of different possibilities for I and J. It would be reasonable to allow H to depend on the value of $||u||$ and, therefore, to revise the above bound so that the second factor is part of the summand; however, doing so will not lead to an improvement in the results we are establishing.

We show next, as promised, that if H is chosen appropriately, then for each primary $u \in R$ with $||u|| > T^{1/n}$, there is at most one $v \in R$ such that $u^k v = E(a - \gamma b)$ for some rational integers $a \in I$ and $b \in J$. Assume otherwise, and fix a primary number $u \in R$ with $||u|| > T^{1/n}$, v_1 and $v_2 \in R$ with $v_1 \neq v_2$, and rational integers $a_1, a_2 \in I$ and $b_1, b_2 \in J$ such that $u^k v_j = E(a_j - \gamma b_j)$ for $j = 1$ and 2. Since u is primary, $|N(u)| \gg ||u||^n$. Thus,

$$|\sigma(u)| \geq \frac{|N(u)|}{||u||^{n-1}} \gg ||u|| \gg T^{1/n} \qquad \text{for every } \sigma \in \{\sigma_1, \dots, \sigma_n\}.$$

Since v_1 and $v_2 \in R$ with $v_1 \neq v_2$, we get that there is a $\sigma \in \{\sigma_1, \dots, \sigma_n\}$ such that $|\sigma(v_1 - v_2)| \geq 1$. Hence,

$$T^{k/n} \ll \left|\sigma(u^k)\right| \left|\sigma\left(v_1 - v_2\right)\right| = \left|\sigma\left(u^k v_1 - u^k v_2\right)\right| = |\sigma(E)| \left|(a_1 - a_2) - \gamma(b_1 - b_2)\right|.$$

Recalling the the a_j and b_j are in intervals of length $\leq H$, we get that $T^{k/n} \ll H$. Hence, we get that there is some sufficiently small constant c_3 such that the condition

$$H \leq c_3 T^{k/n} \tag{1}$$

leads to a contradiction and, hence, also implies the uniqueness of $v \in R$ as described above.

Lemma 3. *Let $t \geq 1$, and let $u \in R$. Let $u_1, u_2, \dots, u_n$ be rational integers such that*

$$u = u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n.$$

Then

$$|u_j| \ll ||u|| \quad \text{for } j \in \{1, 2, \dots, n\},$$

where the implied constant depends on n and the choice of the integral basis $\{\omega_1, \dots, \omega_n\}$.

Proof. Let $\{\omega_1^*, \dots, \omega_n^*\}$ be the dual basis of the basis $\{\omega_1, \dots, \omega_n\}$. Thus,

$$u_j = \sum_{i=1}^{n} \sigma_i(\omega_j^* u) \quad \text{for each } j \in \{1, \dots, n\}.$$

Since $||\omega_j^*|| \ll 1$, we get that

$$|u_j| = \left| \sum_{i=1}^{n} \sigma_i(\omega_j^* u) \right| \leq \sum_{i=1}^{n} |\sigma_i(\omega_j^*)| \, |\sigma_i(u)| \leq \sum_{i=1}^{n} ||\omega_j^*|| \, ||u|| \ll ||u||,$$

completing the proof.

To estimate $|\mathcal{S}(t)|$, we consider cubes $C(t)$ in $\mathbb{Z}^n$ defined by

$$C(t) = \left\{ (u_1, \dots, u_n) : u_j \in \mathbb{Z} \text{ and } |u_j| \leq 2c_4 t^{1/n} \text{ for } j = 1, \dots, n \right\},$$

where c_4 is the implied constant in Lemma 3. Thus, if $u \in \mathcal{S}(t)$, then $u = u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n$ where $(u_1, \dots, u_n) \in C(t)$. Observe that with u so chosen and $\sigma \in \{\sigma_1, \dots, \sigma_n\}$, we get that

$$(2) \qquad |\sigma(u)| = |\sigma(u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n)| = \left| \sum_{j=1}^{n} u_j \sigma(\omega_j) \right| \ll \max_{1 \leq j \leq n} |u_j|.$$

This means that with $u \in \mathcal{S}(t)$, we cannot have that $|u_j|$ is small for every $j \in \{1, \dots, n\}$ (as small as $c_5 t^{1/n}$ for some sufficiently small c_5). Thus, the cube $C(t)$ contains a smaller cube with $n-$tuples which do not correspond to $u \in \mathcal{S}(t)$. It is not really to our advantage to take this into account; however, we will make use of (2) momentarily. We will find r cubes $C_j = C_j(t)$ with $C = \cup_{j=1}^r C_j$ and such that each C_j contains $\ll 1$ $n-$tuples $(u_1, \dots, u_n)$ with $u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n \in \mathcal{S}(t)$. It will then follow that

$$|\mathcal{S}(t)| \ll r \ll \frac{|C(t)|}{\min_{1\le j\le r} |C_j|} \ll \frac{t}{\min_{1\le j\le r} |C_j|}.$$

Fix H satisfying (1) and intervals I and J as before. For each $u \in \mathcal{S}(t)$, we denote by $v(u) \in R$, $a(u) \in I$, and $b(u) \in J$ numbers satisfying

$$E\left(a(u) - \gamma b(u)\right) = u^k v(u).$$

Now, fix $u \in \mathcal{S}(t)$. For each $\alpha \in R$ with $u + \alpha \in \mathcal{S}(t)$, we have that

$$E\left(a(u+\alpha) - \gamma b(u+\alpha)\right) = (u+\alpha)^k\, v(u+\alpha).$$

Since $u \in \mathcal{S}(t)$, we have that u is primary and that $t^{1/n} < ||u|| \le 2t^{1/n}$. Thus,

$$|\sigma(u)| \ge \frac{|N(u)|}{||u||^{n-1}} \gg ||u|| \gg t^{1/n} \qquad \text{for every } \sigma \in \{\sigma_1, \dots, \sigma_n\}.$$

Therefore, there is a constant c_6 such that

$$c_6 t^{1/n} < |\sigma(u)| \le 2t^{1/n} \tag{3}$$

for every $\sigma \in \{\sigma_1, \dots, \sigma_n\}$.

Lemma 4. *Let s be a non-negative integer $\le k-1$. There exist polynomials $P_s = P_s(u,\alpha)$ and $Q_s = Q_s(u,\alpha)$ satisfying:*

(i) P_s and Q_s are homogeneous polynomials in $\mathbb{Z}[u,\alpha]$ of degree s.

(ii) $(u+\alpha)^k P_s - u^k Q_s$ is a polynomial of degree $k-s-1$ in the variable u (and, hence, divisible by α^{2s+1}).

(iii) The coefficient of α^s in P_s is $(-1)^s(k-1)!/(k-s-1)!$, and the coefficient of α^s in Q_s is $(k+s)!/k!$.

In the case that $s = k-1$, the polynomials in Lemma 3 were first considered by Halberstam and Roth [7]. In the general form, they were first used by Nair [10,11] and later by Huxley and Nair [9]. The author [2] made further use of the polynomials in the special cases $s = k-2$ and $s = k-3$ (combined with the Halberstam and Roth polynomials with $s = k-1$). Recently, Trifonov [13] has discussed consequences of the general case in his work on the gap problem for $k-$free numbers. The coefficients of the polynomials in the general case were first determined in the work of Huxley and Nair [9]. In particular the information listed in the statement of Lemma 4 can be found there, but a couple of minor observations are worth mentioning. First, their polynomials were written in a slightly different form. Second, the comment about the degree with respect to the variable u in (ii) is not mentioned explicitly; instead they only mention (and only needed) $k-s-1$ as an upper bound on the degree, but it is easy to get this additional information from their work. We omit the proofs, but note that an alternative approach and some further polynomials with similar properties can be found in [3].

3. The Proof of the Theorem

In this section, we show how Nair's analog of the Halberstam and Roth method for algebraic number fields (cf. [10, 11]) results in the theorem. Our discussion follows closely the description of the Halberstam and Roth method given in [2]. Throughout this section, we consider $k \le n-1$. We return to viewing u as a fixed element of $\mathcal{S}(t)$, and recall the discussion preceding Lemma 4 so that, in particular, a and b are functions of u with $a \in I$ and $b \in J$ for some subintervals I and J of $[1, X]$ of lengths $\le H$. We also fix Y to be some number of the form $a' - \gamma b'$ with $a' \in I$ and $b' \in J$, and observe that

$$\sigma(Y) \ll X \qquad \text{for all } \sigma \in \{\sigma_1, \dots, \sigma_n\}.$$

Since for any $\sigma \in \{\sigma_1, \dots, \sigma_n\}$ and any $\alpha \in R$,

$$|(a(u+\alpha) - \sigma(\gamma) b(u+\alpha)) - \sigma(Y)| \le |a(u+\alpha) - a'| + |\sigma(\gamma)||b(u+\alpha) - b'| \ll H,$$

we get that

$$\frac{a(u+\alpha) - \sigma(\gamma) b(u+\alpha)}{\sigma(u+\alpha)^k} = \frac{\sigma(Y)}{\sigma(u+\alpha)^k} + O\left(H/|\sigma(u+\alpha)|^k\right).$$

Note that the above holds for any $u+\alpha \in \mathcal{S}(t)$ so that, in particular, it holds with $\alpha = 0$. Consider now a fixed α with $u+\alpha \in \mathcal{S}(t)$. Observe that since u and $u+\alpha \in \mathcal{S}(t)$,

$$|\sigma(\alpha)| = |\sigma(u+\alpha) - \sigma(u)| \le |\sigma(u+\alpha)| + |\sigma(u)| \le 4t^{1/n}.$$

Actually, we will be restricting our attention to u and $u+\alpha$ corresponding to elements in a cube $C_j(t)$ as described earlier and will be able to get a better upper bound for $|\sigma(\alpha)|$, but the above estimate will serve our immediate purposes. With $P_s = P_s(u,\alpha)$ and $Q_s = Q_s(u,\alpha)$ as in Lemma 4, we get that $v(u)P_s - v(u+\alpha)Q_s$ is an algebraic integer in K so that there is a $\sigma \in \{\sigma_1, \dots, \sigma_n\}$ (depending on u, α, and s) such that

$$v(u)P_s - v(u+\alpha)Q_s = 0 \quad \text{or} \quad |\sigma(v(u)P_s - v(u+\alpha)Q_s)| \ge 1. \tag{4}$$

We fix such a σ. Using (3) and the definitions of $a(u+\alpha)$, $b(u+\alpha)$, and $v(u+\alpha)$, we obtain that

$$\begin{aligned}
(5) \quad & \sigma\left(v(u)P_s - v(u+\alpha)Q_s\right) \\
&= \frac{\sigma(E)\left(a(u) - \sigma(\gamma)b(u)\right)}{\sigma(u)^k} P_s(\sigma(u),\sigma(\alpha)) \\
&\qquad\qquad - \frac{\sigma(E)\left(a(u+\alpha) - \sigma(\gamma)b(u+\alpha)\right)}{\sigma(u+\alpha)^k} Q_s(\sigma(u),\sigma(\alpha)) \\
&= \frac{\sigma(E)\sigma(Y)}{\sigma(u)^k} P_s(\sigma(u),\sigma(\alpha)) - \frac{\sigma(E)\sigma(Y)}{\sigma(u+\alpha)^k} Q_s(\sigma(u),\sigma(\alpha)) \\
&\qquad\qquad + O\left(\frac{\max\{|\sigma(u)|, |\sigma(\alpha)|\}^s H}{\min\{|\sigma(u)|, |\sigma(u+\alpha)|\}^k}\right) \\
&= \sigma(E)\sigma(Y) \frac{(\sigma(u)+\sigma(\alpha))^k P_s(\sigma(u),\sigma(\alpha)) - \sigma(u)^k Q_s(\sigma(u),\sigma(\alpha))}{\sigma(u)^k(\sigma(u)+\sigma(\alpha))^k} + O\left(H/t^{(k-s)/n}\right).
\end{aligned}$$

The main term above involves the expression

$$L = L\left(\sigma(u),\sigma(\alpha)\right) = (\sigma(u)+\sigma(\alpha))^k P_s(\sigma(u),\sigma(\alpha)) - \sigma(u)^k Q_s(\sigma(u),\sigma(\alpha)).$$

The purpose of the polynomials P_s and Q_s is to control the size of this expression while at the same time not allowing the error term to get too large. The influence of the polynomials to the error term is the $-s$ occuring in the exponent of t. The smaller s is the smaller the error term will be. On the other hand, as will be clearer shortly, larger values of s will make L smaller. Observe that by Lemma 4 (ii), L is a polynomial of degree $k-s-1$ in $\sigma(u)$ and L is divisible by $\sigma(\alpha)^{2s+1}$.

We now show how to use (5) to establish that if $C_1(t)$ is a sub-cube of $C(t)$ with edge length

$$\leq c_7 X^{-1/(2s+1)} t^{(k+s+1)/(n(2s+1))},$$

then the number of $n-$tuples $(u_1,\ldots,u_n)$ in $C_1(t)$ with $u_1\omega_1+\cdots+u_n\omega_n\in\mathcal{S}(t)$ is $\leq 2s$. Here we will choose c_7 to be a sufficiently small constant. Assume that such a $C_1(t)$ exists with $> 2s\geq 2$ such $n-$tuples. Let $u=u_1\omega_1+\cdots+u_n\omega_n$, $\alpha=a_1\omega_1+\cdots+a_n\omega_n$, and $\beta=b_1\omega_1+\cdots+b_n\omega_n$ be such that u, $u+\alpha$, and $u+\alpha+\beta\in\mathcal{S}(t)$ and $(u_1,\ldots,u_n)$, $(u_1+a_1,\ldots,u_n+a_n)$, and $(u_1+a_1+b_1,\ldots,u_n+a_n+b_n)\in C_1(t)$. Then for $j\in\{1,\ldots,n\}$, we get that

$$|a_j|\leq c_7 X^{-1/(2s+1)} t^{(k+s+1)/(n(2s+1))}$$

and

$$|b_j|\leq c_7 X^{-1/(2s+1)} t^{(k+s+1)/(n(2s+1))}.$$

Since $u\in\mathcal{S}(t)$ and $a(u)$ and $b(u)\in[1,X]$, we get by taking norms of both sides of the equation $E\left(a(u)-\gamma b(u)\right)=u^k v(u)$ that

$$t^{k/n}\ll X.$$

Thus, since we are considering $k\leq n-1$,

$$\begin{aligned}(6)\qquad \max\left\{|\sigma(\alpha)|,|\sigma(\beta)|\right\} &\ll c_7 X^{-1/(2s+1)} t^{(k+s+1)/(n(2s+1))}\\ &\ll t^{(s+1)/(n(2s+1))}=o\left(t^{1/n}\right).\end{aligned}$$

Although we are viewing σ as fixed so that (4) holds, observe for future purposes that (6) is true with σ replaced by any homomorphism of K fixing $\mathbb{Q}$. From (3), we can view $|\sigma(u)|$ as being considerably larger than $|\sigma(\alpha)|$ and $|\sigma(\beta)|$. We deduce from Lemma 4 that

$$L \ll |\sigma(u)|^{k-s-1} \, |\sigma(\alpha)|^{2s+1}.$$

Thus, by (3), (5), and (6), we obtain that

$$\begin{aligned}\sigma(v(u)P_s - v(u+\alpha)Q_s) &\ll \frac{|\sigma(\alpha)|^{2s+1} X}{|\sigma(u)|^{k+s+1}} + O\left(H/t^{(k-s)/n}\right) \\ &\ll c_7^{2s+1} \frac{\left(X^{-1/(2s+1)} t^{(k+s+1)/(n(2s+1))}\right)^{2s+1} X}{t^{(k+s+1)/n}} + O\left(H/t^{(k-s)/n}\right) \\ &\ll c_7^{2s+1} + O\left(H/t^{(k-s)/n}\right),\end{aligned}$$

where we have indicated above only the dependence on c_7 in the constants. In particular, the constant c_6 appears as part of the implied constant. We choose

$$H = c_8 T^{(k-s)/n},$$

where c_8 is sufficiently small. Then (1) holds. Having already fixed c_6, we are now in a position to fix c_7 in such a manner that the last expression above has absolute value < 1; in other words, we get that

$$|\sigma\left(v(u)P_s - v(u+\alpha)Q_s\right)| < 1.$$

By (4), we now obtain that

$$v(u)P_s(u,\alpha) - v(u+\alpha)Q_s(u,\alpha) = 0. \tag{7}$$

Observe that the above identity holds whenever u and $u+\alpha$ are in $\mathcal{S}(t)$ and their corresponding $n-$tuples are in $C_1(t)$. Therefore, we also get that

$$v(u)P_s(u,\alpha+\beta) - v(u+\alpha+\beta)Q_s(u,\alpha+\beta) = 0$$

and

$$v(u+\alpha)P_s(u+\alpha,\beta) - v(u+\alpha+\beta)Q_s(u+\alpha,\beta) = 0.$$

Using these last 2 identities, we obtain that

$$v(u)P_s(u,\alpha+\beta)Q_s(u+\alpha,\beta) - v(u+\alpha)P_s(u+\alpha,\beta)Q_s(u,\alpha+\beta) = 0$$

so that from the first identity we get that

$$v(u)\left(P_s(u,\alpha)P_s(u+\alpha,\beta)Q_s(u,\alpha+\beta) - P_s(u,\alpha+\beta)Q_s(u+\alpha,\beta)Q_s(u,\alpha)\right) = 0.$$

Since $E(a(u) - \gamma b(u)) = u^k v(u)$ and γ is a root of an irreducible polynomial of degree $n \geq 2$, we easily get that $v(u) \neq 0$. Hence,

$$P_s(u,\alpha)P_s(u+\alpha,\beta)Q_s(u,\alpha+\beta) - P_s(u,\alpha+\beta)Q_s(u+\alpha,\beta)Q_s(u,\alpha) = 0. \tag{8}$$

We now show that the left-hand side of (8) is a non-zero polynomial in β of degree $2s$. In fact, as a polynomial in β, it follows from Lemma 4 (iii) that the coefficient of β^{2s} on the left-hand side of (8) is

$$\begin{aligned} P_s(u,\alpha)\left((-1)^s\frac{(k-1)!}{(k-s-1)!}\right)\frac{(k+s)!}{k!} - \left((-1)^s\frac{(k-1)!}{(k-s-1)!}\right)\frac{(k+s)!}{k!}Q_s(u,\alpha) \\ = (-1)^s\frac{(k-1)!(k+s)!}{(k-s-1)!k!}\left(P_s(u,\alpha) - Q_s(u,\alpha)\right). \end{aligned}$$

The inequality in (6) holds with σ replaced by the identity homomorphism so that $|\alpha|$ is small compared to $|u|$. It is easy to establish, therefore, that $P_s(u,\alpha) \neq 0$. Now, if $P_s(u,\alpha) = Q_s(u,\alpha)$, then it would follow from (7) that $v(u+\alpha) = v(u)$ and, hence, that

$$\begin{aligned} E((a(u+\alpha) - a(u)) - &\gamma(b(u+\alpha) - b(u))) \\ &= E\left(a(u+\alpha) - \gamma b(u+\alpha)\right) - E\left(a(u) - \gamma b(u)\right) \\ &= \left((u+\alpha)^k - u^k\right)v(u) \\ &= \left(ku^{k-1} + \frac{k(k-1)}{2}\alpha u^{k-2} + \cdots\right)\alpha v(u). \end{aligned}$$

Note that there is a homomorphism $\sigma_j \in \{\sigma_1, \dots, \sigma_n\}$ such that $|\sigma_j(\alpha v(u))| \geq 1$. If we apply such a homomorphism to the equation above, we get that the right-hand side will be $\gg |u|^{k-1} \gg t^{(k-1)/n}$. Also, since $a(u+\alpha)$ and $a(u) \in I$ and $b(u+\alpha)$ and $b(u) \in J$ with $|I|$ and $|J|$ each $\leq H$, the left-hand side will be $\ll H$. We will take $s \geq 1$ so that the above is impossible. Thus, we get that the left-hand side of (8) is a non-zero polynomial in β of degree $2s$. Hence, there are at most $2s$ possible values of β as above including $\beta = 0$ and $\beta = -\alpha$. In other words, with $s \geq 1$, there are $\leq 2s$ different $u = u_1\omega_1 + \cdots + u_n\omega_n \in \mathcal{S}(t)$ with $(u_1, \dots, u_n) \in C_1(t)$. We divide $C(t)$ into as few sub-cubes as possible with each edge length $\leq c_7 X^{-1/(2s+1)} t^{(k+s+1)/(n(2s+1))}$. Recall that $t \ll X^{n/k}$. By the above and our previous comments, we obtain that

$$\begin{aligned} |\mathcal{S}(t)| &\ll \frac{t}{c_7^n X^{-n/(2s+1)} t^{(k+s+1)/(2s+1)}} + 1 \\ &\ll X^{n/(2s+1)} t^{(s-k)/(2s+1)}, \end{aligned} \tag{9}$$

(where now the implied constant depends on c_7). In our upper bound for $P(X)$, we can therefore take $B(X,t)$ to be the last expression in (9). Recalling from Lemma 3, we will need $s \leq k-1$, we obtain that

$$P(X) \ll X^{n/(2s+1)} T^{-(k-s)/(2s+1)} \left(\frac{X}{H} + 1 \right)^2 .$$

Except for the power of 2 appearing in this last factor, this bound for $P(X)$ is the same bound one gets in the single variable problem (cf. [10, 11]). Recall that $1 \leq s \leq k-1$, $H = c_8 T^{(k-s)/n}$, and $T = X^2$. Observe that by definition, $P(X) = 0$ unless there exist integers a and b in $[1, X]$ such that $p^k | f(a,b)$ for some prime $p > T$. But this means

$$X^{2k} = T^k < p^k \leq f(a,b) \ll X^n,$$

where we have used that $f(a,b) \neq 0$ since $f(x,y)$ is irreducible and of degree ≥ 2. Thus, $P(X) = 0$ if $k > n/2$, and the theorem trivially follows from Lemma 1. In fact, it is not difficult to modify this simple observation to deal with the case that $f(x,y)$ is of degree 1. Consider now the case that $k \leq n/2$. Then one easily gets $H \leq X$. We deduce that

$$P(X) \ll X^r,$$

where

$$r = 2 + \frac{n+2s-2k}{2s+1} - \frac{4k-4s}{n}.$$

To obtain an asymptotic result from Lemma 1, we require $r < 2$. In other words, we need

$$n(n+2s-2k) - (2s+1)(4k-4s) < 0.$$

We expand the left-hand side and complete a square to reduce the problem to showing that

$$\frac{1}{2}\left(4s - \frac{4k-n-2}{2}\right)^2 + \frac{1}{8}\left(7n^2 - 16k^2 - 8kn - 4n - 16k - 4\right) < 0$$

To simplify matters, we only consider $n \geq 8$; the remaining n can be dealt with similarly. We consider $k \geq (2\sqrt{2}-1)n/4$. For such k and n, we have that $(4k-n-2)/2 \geq 2$ and $k \geq 2$. Also, one checks that $4(k-1) \geq (4k-n-2)/2$. We conclude that there is an $s \in \{1, 2, \ldots, k-1\}$ such that the multiple $4s$ of 4 is within 2 of $(4k-n-2)/2$. Hence, using this choice for s, we need only show that

$$2 + \frac{1}{8}\left(7n^2 - 16k^2 - 8kn - 4n - 16k - 4\right) < 0.$$

Since the left-hand side is a decreasing function of k and $k \geq (2\sqrt{2}-1)n/4$, we will be through if the value of the left-hand side is < 0 when we replace k with $(2\sqrt{2}-1)n/4$. Doing so, the left-hand side becomes $(3 - 2\sqrt{2}n)/2$, giving the desired result. Thus, we have established the theorem in the case that $n \geq 8$.

4. Further Remarks

In this section, we make some remarks concerning improvements on the theorem in the introduction. In Gouvêa and Mazur [4], they made the nice observation that Hooley's method can be used to obtain results about $k-$free values of reducible polynomials $f(x) \in \mathbb{Z}[x]$ and $k-$free values of reducible binary forms $f(x,y) \in \mathbb{Z}[x,y]$. More specifically, in the case that $f(x) \in \mathbb{Z}[x]$, one can show that if $f(x)$ is squarefree with no fixed kth prime power divisor and each irreducible factor of $f(x)$ has degree $\leq k+1$, then there are infinitely many integers m for which $f(m)$ is $k-$free and the density of such m is $\prod_p \left(1-(\rho(p^k)/p^k)\right)$. From the work of Greaves [6], one gets that if $f(x,y)$ is a squarefree binary form of degree n with non-zero coefficients for x^n and y^n which has no fixed kth prime power divisor and if the degree of each irreducible factor of $f(x,y)$ is ≤ 6 in the case $k=2$ and is $\le 2k+1$ in the case of $k>2$, then there are infinitely many integer pairs (a,b) for which $f(a,b)$ is $k-$free and the density of such pairs is $\prod_p \left(1-(\rho(p^k)/p^{2k})\right)$. The analogous extensions of Nair's method hold for both the single variable problem and the binary form problem. To explain these comments briefly, we consider the case of a binary form $f(x,y)$ and we refer back to the proof of Lemma 1. We considered there three quantities S_1, S_2, and S_3. One checks that the estimates given for S_1 remain valid when $f(x,y)$ is reducible as above. Observe here, though, that the other assumptions made are essential. For example, we must have $f(x,y)$ squarefree or else $\Delta=0$ and our bounds on $\rho(p^k)$ need revising and $\prod_p \left(1-(\rho(p^k)/p^{2k})\right)=0$. For S_2 and S_3, one works separately with the contribution of each irreducible factor of $f(x,y)$ and then pieces them together (cf. [4],[6]). (We avoided the situation that $\deg f=1$ in the previous sections, but it is not difficult to deal with factors of degree one as well.) The difference between Hooley's method and Nair's is in the estimating of S_3, but in either case, one can piece together the contribution of each irreducible factor provided $f(x,y)$ is squarefree.

Suppose now that N_f denotes the greatest common divisor of the values of $f(m)$ if $f(x)\in\mathbb{Z}[x]$ and of $f(a,b)$ if $f(x,y)\in\mathbb{Z}[x,y]$. In either case, denote the degree of f by n. In the case that $f(x)\in\mathbb{Z}[x]$, Hensel (cf. [1]) showed that one can compute N_f from

$$N_f=\gcd(f(0),f(1),\dots,f(n)).$$

It is fairly easy to conclude from the situation in one variable, that in the binary case

$$N_f=\gcd\left(f(i,j):i,j\in\{0,1,\dots,n\}\right).$$

We factor N_f as U_fV_f where V_f is the largest k-free factor of N_f. We observe that it is possible to replace the role of $f(x)$ and $f(x,y)$ in the results obtained from Hooley's and Nair's methods by $f(x)/U_f$ and $f(x,y)/U_f$; then one needn't require that f has no fixed kth prime power divisor. Thus, for example, if $f(x,y)$ is a squarefree binary form of degree n with non-zero coefficients for x^n and y^n with each irreducible factor of $f(x,y)$ of degree $\leq 4k/(2\sqrt{2}-1)$, then there are infinitely many integer pairs (a,b) for which $f(a,b)$ is $k-$free and the density of such pairs is

$$\prod_{p\nmid U_f}\left(1-(\rho(p^k)/p^{2k})\right)\prod_{p^r\,||U_f}\left(1-(\rho(p^{k+r})/p^{2k+2r})\right).$$

It is perhaps worth noting that one has as an example that for any non-negative integer n, there are infinitely many integers m for which $\binom{m}{n}$ is squarefree and the density of such m is

$$\prod_{p>n}\left(1-\frac{n}{p^2}\right)\prod_{p\leq n}\left(1-\frac{\rho(p^{e(p)})}{p^{e(p)}}\right)$$

where $e(p)=2+[n/p]+[n/p^2]+\cdots$ and $\rho(p^{e(p)})$ is the number of positive integers $u\leq p^{e(p)}$ such that $p^{e(p)}$ divides $u(u+1)\cdots(u+n-1)$. We note, however, that the result in this example is an easy consequence of sieve methods.

As mentioned in the introduction, the constant $(2\sqrt{2}-1)/4$ appearing in the theorem is the best constant that comes out of these methods, but the theorem does not in general give the best k for a given n. For example, a direct application of the theorem suggests that these methods only improve on Greaves' results when $k\geq(2\sqrt{2}-1)(2k+2)/4$ or, in other words, when $k\geq 11$. However, we can obtain $k-$free values for binary forms f (as described above or in the previous sections) of degree $2k+2$ whenever $k\geq 5$ as follows. Take $T=X^2\sqrt{\log X}$. Take $H=c_8T^{(k-s)/n}$ as in Section 3. Recall that

$$P(X)\ll X^{n/(2s+1)}T^{-(k-s)/(2s+1)}\left(\frac{X}{H}+1\right)^2. \tag{10}$$

Since $1\leq s\leq k-1$, one easily checks that $\log X$ appears to a negative exponent on the right-hand side. Thus, to obtain that $f(a,b)$ is $k-$free for infinitely many (a,b), we only need

$$\frac{n+2s-2k}{2s+1}\leq\frac{4k-4s}{n}.$$

Taking $s=1$ and $n=2k+2$, we easily obtain the above inequality whenever $k\geq 5$.

References

1. L.E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1971.
2. M. Filaseta, *An elementary approach to short intervals results for k–free numbers*, J. Number Theory **30** (1988), 208–225.
3. M. Filaseta, *Short interval results for k-free values of irreducible polynomials*, preprint.
4. F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.
5. G. Greaves, *Large prime factors of binary forms*, J. Number Theory **3** (1971), 35–59 *and Corrigendum, ibid.* 9 (1977), 561–562.
6. G. Greaves, *Power-free values of binary forms*, Quarterly J. Math. Oxford (2) **43** (1992), 45–65.
7. H. Halberstam and K. F. Roth, *On the gaps between consecutive k–free integers*, J. London Math. Soc. (2) **26** (1951), 268–273.
8. C. Hooley, *On the power free values of polynomials*, Mathematika **14** (1967), 21–26.
9. M. N. Huxley and M. Nair, *Power free values of polynomials III*, Proc. London Math. Soc. **41** (1980), 66–82.
10. M. Nair, *Power free values of polynomials*, Mathematika **23** (1976), 159–183.
11. M. Nair, *Power free values of polynomials II*, Proc. London Math. Soc. (3) **38** (1979), 353–368.
12. N.S. Sukthankar, *On Grimm's conjecture in algebraic number fields*, Indagationes Mathematicae **35** (1973), 475–484.
13. O. Trifonov, *On gaps between $k-$free numbers*, preprint.

Mathematics Department
University of South Carolina
Columbia, SC 29208