



Universiteit
Leiden
The Netherlands

The abc-conjecture and k-free numbers

Barry, A.

Citation

Barry, A. (2007). *The abc-conjecture and k-free numbers*.

Version: Not Applicable (or Unknown)

License: [License to inclusion and publication of a Bachelor or Master thesis in the Leiden University Student Repository](#)

Downloaded from: <https://hdl.handle.net/1887/3597518>

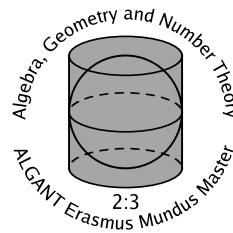
Note: To cite this publication please use the final published version (if applicable).

Amadou Diogo Barry

The abc Conjecture and k -free numbers

Master's thesis, defended on June 20, 2007

Thesis advisor: Dr. Jan-Hendrik Evertse



Mathematisch Instituut
Universiteit Leiden

Exam committee

Dr. Jan-Hendrik Evertse (supervisor)

Prof.dr. P. Stevenhagen

Prof.dr. R. Tijdeman

Abstract

In his paper [\[14\]](#), A. Granville proved several strong results about the distribution of square-free values of polynomials, under the assumption of the abc-conjecture. In our thesis, we generalize some of Granville's results to k -free values of polynomials (i.e., values of polynomials not divisible by the k -th power of a prime) . Further, we generalize a result of Granville on the gaps between consecutive square-free numbers to gaps between integers, such that the values of a given polynomial f evaluated at them are k -free. All our results are under assumption of the abc-conjecture.

Contents

1	Introduction	2
2	The <i>abc</i>-conjecture and some consequences	6
2.1	The <i>abc</i> -conjecture	6
2.2	Consequences of the <i>abc</i> -conjecture	6
3	Asymptotic estimate for the density of integers n for which $f(n)$ is k-free	13
3.1	Asymptotic estimate of integers n for which $f(n)$ is k -free . . .	13
3.2	On gaps between integers at which a given polynomial assumes k -free values	17
4	The average moments of $s_{n+1} - s_n$	19
	Bibliography	27

Notation

Let $f : \mathbb{R} \rightarrow \mathbb{C}$ and $g : \mathbb{R} \rightarrow \mathbb{C}$ be complex valued functions and $h : \mathbb{R} \rightarrow \mathbb{R}^+$. We use the following notation:

$$f(X) = g(X) + O(h(X)) \text{ as } X \rightarrow \infty$$

if there are constants X_0 and $C > 0$ such that

$$|f(X) - g(X)| \leq Ch(X)$$

for all $X \in \mathbb{R}$ and $X \geq X_0$;

$$f(X) = g(X) + o(h(X)) \text{ as } X \rightarrow \infty \text{ iff } \lim_{X \rightarrow \infty} \frac{f(X) - g(X)}{h(X)} = 0;$$

$$f(X) \sim g(X) \text{ as } X \rightarrow \infty \text{ iff } \lim_{X \rightarrow \infty} \frac{f(X)}{g(X)} = 1.$$

We write $f(X) \ll g(X)$ or $g(X) \gg f(X)$ to indicate that $f(X) = O(g(X))$

We denote by $\gcd(a_1, a_2, \dots, a_r)$, $\text{lcm}(a_1, a_2, \dots, a_r)$, the greatest common divisor, and the lowest common multiple, respectively, of the integers

a_1, a_2, \dots, a_r .

We say that a positive integer n is k -free if n is not divisible by the k -th power of a prime number.

Chapter 1

Introduction

In 1985, Oesterlé and Masser posed the following conjecture:

The abc -conjecture. Fix $\varepsilon > 0$. If a, b, c are coprime positive integers satisfying $a + b = c$ then

$$c \ll_{\varepsilon} N(abc)^{1+\varepsilon},$$

where for a given integer m , $N(m)$ denotes the product of the distinct primes dividing m .

In fact, Oesterlé first posed a weaker conjecture, motivated by a conjecture of Szpiro regarding elliptic curves. Then Masser posed the abc -conjecture as stated above motivated by a Theorem of Mason, which gives an similar statement for polynomials.

On its own, the abc -conjecture merits much admiration. Like the most intriguing problems in Number Theory, the abc -conjecture is easy to state but apparently very difficult to prove. The abc -conjecture has many fascinating applications; for instance Fermat's last Theorem, Roth's theorem, and the Mordell conjecture, proved by G. Faltings [4] in 1984.

Another consequence is the following result proved by Langevin [22] and Granville [14]:

Assume that the abc -conjecture is true. Let $F(X, Y) \in \mathbb{Q}[X, Y]$ be a homogeneous polynomial of degree $d \geq 3$, without any repeated linear factor such that $F(m, n) \in \mathbb{Z}$ for all $m, n \in \mathbb{Z}$. Fix $\varepsilon > 0$. Then, for any coprime integers m and n ,

$$N(F(m, n)) \gg \max\{|m|, |n|\}^{d-2-\varepsilon},$$

where the constant implied by \gg depends only on ε and F . With this consequence we generalize some results of Granville [14] on the distribution problem for the square free values of polynomials to the distribution problem for k -free values of polynomials for every $k \geq 2$.

Let $f(X) \in \mathbb{Q}[X]$ be a non-zero polynomial without repeated roots such that $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

In his paper, Granville proved, under the *abc*-conjecture assumption, that if $\gcd_{n \in \mathbb{Z}}(f(n))$ is square free, then there are asymptotically $c_f N$ positive integers $n \leq N$ such that $f(n)$ is square free, where c_f is a positive constant depending only on f .

In section 3.1, we generalize this as follows:

Assume the abc-conjecture. Let k be an integer ≥ 2 and suppose that $\gcd_{n \in \mathbb{Z}}(f(n))$ is k -free. Then there is a positive constant $c_{f,k}$ such that:

$$\#\{n \in \mathbb{Z} : n \leq N, \quad f(n) \text{ } k\text{-free}\} \sim c_{f,k} N \quad \text{as } N \rightarrow \infty$$

If we do not assume the *abc*-conjecture only under much stronger constraints results have been proved. For example Hooley [18] obtained only the following result.

Let $f(X)$ be an irreducible polynomial of degree $d \geq 3$ for which $\gcd_{n \in \mathbb{Z}} f(n)$ is $(d-1)$ -free. Then if $S(x)$ is the number of positive integers $\leq x$ for which $f(n)$ is $(d-1)$ -free, we have as $x \rightarrow \infty$

$$S(x) = x \prod_p \left(1 - \frac{\omega_f(p)}{p^{d-1}}\right) + O\left(\frac{x}{(\log x)^{A/\log \log \log x}}\right),$$

where $\omega_f(p) = \#\{0 \leq n < p^{d-1} : f(n) \equiv 0 \pmod{p^{d-1}}\}$ and A is a positive constant depending only on f .

In section 3.2 we will investigate the problem of finding an $h = h(x)$ as small as possible such that, for x sufficiently large, there is an integer $m \in (x, x + h]$ such that $f(m)$ is k -free, where $f(X) \in \mathbb{Q}[X]$ is irreducible and $f(n) \in \mathbb{Z}$ for every $n \in \mathbb{Z}$.

This problem has been investigated in the case $f(X) = X$ and $k = 2$ by Roth [26], and Filaseta and Trifonov [10]. In particular Filaseta and Trifonov have shown in 1990 that there is a constant $c > 0$ such that, for x sufficiently large, the interval $(x, x + h]$ with $h = cx^{8/37}$ contains a square free number. Using exponential sums, they showed that $8/37$ may be replaced by $3/14$. A few years later, in 1993, the same authors obtained the following improvement: there exists a constant $c > 0$ such that for x sufficiently large the interval $(x, x + cx^{1/3} \log x]$ contains a square free number. Under the *abc*-conjecture, Granville [14] showed that $h(x) = x^\varepsilon$ ($\varepsilon > 0$ arbitrary) can be taken.

Again assuming the *abc*-conjecture we extend this as follows:

For every $\varepsilon > 0$ and every sufficiently large x , there is an integer $m \in (x, x + x^\varepsilon]$ such that $f(m)$ is k -free.

Now, let s_1, s_2, \dots denote the positive integers m in ascending order such that $f(m)$ is k -free.

The main purpose of chapter 4 is to study the average moments of $s_{n+1} - s_n$; that is, the asymptotic behaviour of $\frac{1}{x} \sum_{s_{n+1} \leq x} (s_{n+1} - s_n)^A$ as $x \rightarrow \infty$.

It was Erdős [5] who began to study this problem in the case $f(X) = X$. Erdős showed that, if $0 \leq A \leq 2$, then

$$\sum_{s_{n+1} \leq x} (s_{n+1} - s_n)^A \sim \beta_A x \quad \text{as } x \rightarrow \infty \quad (1.1)$$

where β_A is a function depending only on A . In 1973 Hooley[19] extended the range of validity of this result to $0 \leq A \leq 3$; and in 1993, Filaseta [9] extended this further to $0 \leq A < 29/9 = 3,222\dots$

In our case we will allow any $A > 0$ and generalize this result to every irreducible polynomial $f(X) \in \mathbb{Q}[X]$ such that $f(n)$ is an integer for every $n \in \mathbb{Z}$. Before we state our Theorem we recall the result obtained by Beasley and Filaseta [1] without the assumption of the *abc*-conjecture.

Let $d = \deg(f) \geq 2$, and let $k \geq (\sqrt{2} - 1/2)d$. Let

$$\phi_1 = \frac{(2s + d)(k - s) - d(d - 1)}{(2s + d)(k - s) + d(2s + 1)},$$

where

$$s = \begin{cases} 1 & \text{if } 2 \leq d \leq 4 \\ [(\sqrt{2} - 1) d/2] & \text{if } d \geq 5 \end{cases}$$

Let

$$\phi_2 = \begin{cases} \frac{8d(d-1)}{(2k+d)^2-4} & \text{if } (\sqrt{2} - 1/2) \leq k \leq d \\ \frac{d}{(2k-d+r)} & \text{if } k \geq d + 1, \end{cases}$$

where r is the largest positive integer such that $r(r - 1) < 2d$. Then $\phi_1 > 0$, $\phi_2 > 0$,

and if

$$0 \leq A < \min \left\{ \frac{1}{\phi_2}, 1 + \frac{\phi_1}{\phi_2}, k \right\},$$

then for every irreducible polynomial $f(X) \in \mathbb{Z}[X]$ of degree d such that $\gcd_{n \in \mathbb{Z}} f(n)$ is k -free,

$$\sum_{s_{n+1} \leq x} (s_{n+1} - s_n)^A \sim \beta_A x \quad \text{as } x \rightarrow \infty$$

for some constant β_A depending only on A , $f(x)$, and k .

Assuming the *abc*-conjecture we establish the following result, which was

proved by Granville [14] in the special case $f(X) = X, k = 2$:

Let k be an integer $\geq \min(3, \deg(f))$. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial without any repeated root such that $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$ and $\gcd_{n \in \mathbb{Z}} f(n)$ is k -free. Suppose the abc-conjecture is true. Then for every real $A > 0$ there exists a constant $\beta_A > 0$ such that:

$$\sum_{s_n \leq x} (s_{n+1} - s_n)^A \sim \beta_A x \quad \text{as } x \rightarrow \infty.$$

Chapter 2

The *abc*-conjecture and some consequences

2.1 The *abc*-conjecture

We recall the *abc*-conjecture.

The *abc*-conjecture [Oesterlé, Masser, Szpiro].

Fix $\varepsilon > 0$. If a, b, c are coprime positive integers satisfying $a + b = c$ then

$$c \ll_{\varepsilon} N(abc)^{1+\varepsilon},$$

where for a given integer m , $N(m)$ denotes the product of the distinct primes dividing m .

2.2 Consequences of the *abc*-conjecture

Now we state a consequence of the *abc*-conjecture, obtained independently by Granville [14] and Langevin [22] [23], on which all our results will rely.

Theorem 2.1. *Assume that the *abc*-conjecture is true. Let $F(X, Y) \in \mathbb{Q}[X, Y]$ be a homogeneous polynomial of degree $d \geq 3$, without any repeated linear factor such that $F(m, n) \in \mathbb{Z}$ for all $m, n \in \mathbb{Z}$. Fix $\varepsilon > 0$. Then, for any coprime integers m and n ,*

$$N(F(m, n)) \gg \max\{|m|, |n|\}^{d-2-\varepsilon},$$

where the constant implied by \gg depends only on ε and F .

The proof of this Theorem depends on some Lemmas which we state after giving some definitions.

Let $\varphi(z) = \frac{f(z)}{g(z)}$ a rational function, where $f(z), g(z) \in \mathbb{C}[z]$ are coprime polynomials. We define $\deg(\varphi) = \max(\deg(f), \deg(g))$.

φ defines a map from $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ to $\mathbb{P}^1(\mathbb{C})$ by defining:

- (i) $\varphi(z) = \infty$ if $z \neq \infty, g(z) = 0$;
- (ii) $\varphi(\infty) = \infty$ if $\deg(f) > \deg(g)$;
- (iii) $\varphi(\infty) = 0$ if $\deg(f) < \deg(g)$;
- (iv) $\varphi(\infty) = \text{lc}(f)/\text{lc}(g)$ if $\deg(f) = \deg(g)$,

where $\text{lc}(f)$ denotes the leading coefficients of a polynomial f .

We define the multiplicity, $\text{mult}_{z_0}(\varphi)$ of φ at $z_0 \in \mathbb{P}^1(\mathbb{C})$ as follows:

- if $z_0 \neq \infty, \varphi(z_0) \neq \infty$ we define $\text{mult}_{z_0}(\varphi)$ to be the integer n such that $\varphi(z) - \varphi(z_0) = c(z - z_0)^n + (\text{higher power of } (z - z_0))$ and $c \neq 0$;
- if $z_0 \neq \infty, \varphi(z_0) = \infty$, define $\text{mult}_{z_0}(\varphi) = \text{mult}_{z_0}\left(\frac{1}{\varphi}\right)$;
- if $z_0 = \infty$, define $\text{mult}_{z_0}(\varphi) = \text{mult}_{z_0}(\varphi^*)$ where $\varphi^*(z) = \varphi\left(\frac{1}{z}\right)$.

We say that φ is ramified at z_0 if $\text{mult}_{z_0}(\varphi) > 1$.

We say that φ is ramified over w_0 if there is $z_0 \in \mathbb{P}^1(\mathbb{C})$ with $\varphi(z_0) = w_0$ such that φ is ramified at z_0 .

In general we have $\sum_{z_0 \in \varphi^{-1}(w_0)} \text{mult}_{z_0}(\varphi) = \deg(\varphi)$ for $w_0 \in \mathbb{P}^1(\mathbb{C})$.

The following is a special case of the Riemann-Hurwitz formula:

Lemma 2.2. *Let $\varphi \in \mathbb{C}(z)$ be a rational function. Then:*

$$2 \deg(\varphi) - 2 = \sum_{z_0 \in \mathbb{P}^1(\mathbb{C})} (\text{mult}_{z_0}(\varphi) - 1),$$

Proof. For a statement and proof of the general Riemann-Hurwitz formula, see [24] or [29]. □

Let $\overline{\mathbb{Q}}$ denote the algebraic closure of \mathbb{Q} in \mathbb{C} .

Lemma 2.3 (Belyi[2]). *For any finite subset S of $\mathbb{P}^1(\overline{\mathbb{Q}})$, there exists a rational function $\phi(X) \in \mathbb{Q}(X)$, ramified only over $\{0, 1, \infty\}$, such that $\phi(S) \subset \{0, 1, \infty\}$.*

Proof. This useful Lemma is proved, for instance, by Serre as Theorem *B* on page 71 of [28] (for variations, see Belyi [2], Elkies [4], Langevin [22], [23], or Granville [16]). □

Lemma 2.4. *Let $F(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ be any non-zero homogeneous polynomial. Then we can determine a positive integer D , and homogeneous polynomials $a(X, Y), b(X, Y), c(X, Y) \in \mathbb{Z}[X, Y]$ all of degree D , without common factors such that:*

- (i) $a(X, Y)b(X, Y)c(X, Y)$ has exactly $D+2$ non-proportional linear factors, including the factors of F ;
- (ii) $a(X, Y) + b(X, Y) = c(X, Y)$.

Proof. We apply Lemma 2.3 with $S = \{(\alpha, \beta) \in \mathbb{P}^1 : F(\alpha, \beta) = 0\}$. Let $\phi(X)$ be the rational function from Lemma 2.3, and write $\phi(X/Y) = a(X, Y)/c(X, Y)$, where $a(X, Y), c(X, Y) \in \mathbb{Z}[X, Y]$ are homogeneous forms, of the same degree as ϕ , (call it D) and without common factors. Let $b(x, y) = c(x, y) - a(x, y)$. Note that:

$$\begin{aligned} \phi(x/y) = 0 & \quad \text{if and only if} \quad a(x, y) = 0; \\ \phi(x/y) = 1 & \quad \text{if and only if} \quad b(x, y) = 0; \\ \phi(x/y) = \infty & \quad \text{if and only if} \quad c(x, y) = 0. \end{aligned}$$

Therefore $F(x, y)$ divides $a(x, y)b(x, y)c(x, y)$. If we write $\#\phi^{-1}(u)$ for the number of distinct $t \in \mathbb{P}^1(\mathbb{Q})$ for which $\phi(t) = u$, then $\#\phi^{-1}(0) + \#\phi^{-1}(1) + \#\phi^{-1}(\infty)$ equals the number of distinct linear factors of $a(x, y)b(x, y)c(x, y)$, by the observation immediately above. On the other hand, applying the Riemann-Hurwitz formula to the map $\phi : \mathbb{P}^1 \rightarrow \mathbb{P}^1$, and the fact that ϕ is ramified only over $\{0, 1, \infty\}$ we get:

$$\begin{aligned} 2D &= 2 + \sum_{u \in \phi^{-1}(\{0, 1, \infty\})} (\text{mult}_u(\phi) - 1) \\ &= 2 + \sum_{u \in \{0, 1, \infty\}} D - \sum_{u \in \phi^{-1}(\{0, 1, \infty\})} 1 \\ &= 2 + \sum_{u \in \{0, 1, \infty\}} D + \sum_{u \in \{0, 1, \infty\}} \#\phi^{-1}(u) \\ &= 2 + \sum_{u \in \{0, 1, \infty\}} \{D - \#\phi^{-1}(u)\}. \end{aligned}$$

Thus $\#\phi^{-1}(0) + \#\phi^{-1}(1) + \#\phi^{-1}(\infty) = D + 2$ which concludes the proof. \square

Here we give the definition of discriminant, resultant, and some of their properties.

Definition 2.5. *Let, $g(X) = b \prod_{i=1}^r (X - \beta_i) \in \mathbb{Q}[X]$ then we define the discriminant of g by:*

$$\Delta(g) = b^{2r-2} \prod_{1 \leq i < j \leq r} (\beta_i - \beta_j)^2.$$

Definition 2.6. *The resultant of two non-zero polynomials*

$$f(X) = b \prod_{i=1}^s (X - \beta_i), \quad g(X) = c \prod_{j=1}^r (X - \gamma_j) \in \mathbb{Q}[X]$$

is defined by:

$$R(f, g) = b^r c^s \prod_{i=1}^s \prod_{j=1}^r (\beta_i - \gamma_j).$$

We easily deduce from these definitions the following properties:

(R1) $R(f, g) = (-1)^{rs} R(g, f);$

(R2) $R(f, g) = b^r \prod_{i=1}^s g(\beta_i);$

(R3) $\Delta(f) = (-1)^{s(s-1)/2} b^{-1} R(f, f');$

(R4) If $f(X), g(X) \in \mathbb{Z}[X]$, there exist two polynomials $a(X), b(X) \in \mathbb{Z}[X]$ with $\deg(a) \leq r - 1$, $\deg(b) \leq s - 1$ such that:

$$a(X)f(X) + b(X)g(X) = R(f, g).$$

For this last remark see [21] .

Definition 2.7. Let $F(X, Y) = \sum_{i=0}^s a_i X^{s-i} Y^i$, $G(X, Y) = \sum_{j=0}^r b_j X^{r-j} Y^j$ be two binary homogeneous polynomials in $\mathbb{Z}[X, Y]$ such that $a_0 \neq 0$, $b_0 \neq 0$. Then we define the resultant of F and G , $R(F, G)$, by: $R(F, G) = R(f, g)$, where $f(X) = F(X, 1)$ and $g(X) = G(X, 1)$.

Lemma 2.8. Let $F, G \in \mathbb{Z}[X, Y]$ be two binary homogeneous polynomials, without common factor. Let $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. Then:

$$\gcd(F(m, n), G(m, n)) \mid R(F, G).$$

Proof. Let $F(X, Y) = Y^s f\left(\frac{X}{Y}\right)$ and $G(X, Y) = Y^r g\left(\frac{X}{Y}\right)$ then by (R4) there are two polynomials $a(X), b(X) \in \mathbb{Z}[X]$ such that $a(X)f(X) + b(X)g(X) = R(f, g)$. Now put $A(X, Y) = Y^{r-1} a\left(\frac{X}{Y}\right)$, $B(X, Y) = Y^{s-1} b\left(\frac{X}{Y}\right)$. Then

$$A(X, Y)F(X, Y) + B(X, Y)G(X, Y) = Y^{r+s-1} R(F, G).$$

So

$$\gcd(F(m, n), G(m, n)) \mid n^{r+s-1} R(F, G).$$

By interchanging m and n we get:

$$\gcd(F(m, n), G(m, n)) | m^{r+s-1} R(F, G),$$

since $\gcd(m, n) = 1$. Thus,

$$\gcd(F(m, n), G(m, n)) | R(F, G).$$

□

For more details see [21] or [25].

Proof of Theorem 2.1. There is no loss of generality to assume that $F(X, Y) \in \mathbb{Z}[X, Y]$. Let $d = \deg(F)$ and let $a(x, y), b(x, y), c(x, y)$ be the homogeneous polynomials from Lemma 2.4. By multiplying together the irreducible factors of $a(x, y)b(x, y)c(x, y)$, we obtain a new polynomial $F(x, y)G(x, y)$ of degree $D + 2$.

Let $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$ and put $r = \gcd(a(m, n), b(m, n))$. r is bounded since it divides $R(a, b)$ which is a non-zero integer. Now using this remark we apply the abc -conjecture directly to the equation $\frac{a(m, n)}{r} + \frac{b(m, n)}{r} = \frac{c(m, n)}{r}$ to get

$$\max\{|a(m, n)|, |b(m, n)|\} \ll \left(\prod_{p|abc} p \right)^{1+\varepsilon/D},$$

where here and below constants implied by \ll depend on F and ε . This implies:

$$\max\{|a(m, n)|, |b(m, n)|\}^{1-\varepsilon/D} \ll \left(\prod_{p|abc} p \right)^{1-\varepsilon^2/D^2} \leq \left(\prod_{p|abc} p \right);$$

hence

$$\max\{|a(m, n)|, |b(m, n)|\}^{1-\varepsilon/D} \ll \left(\prod_{p|FG} p \right) \ll G(m, n) \left(\prod_{p|F(m, n)} p \right).$$

Now to finish our proof it remains to find an upper bound and a lower bound respectively for $|G(m, n)| = \sum_{i=0}^{D+2-d} g_i m^i n^{D+2-d-i}$ and $\max\{|a(m, n)|, |b(m, n)|\}$.

Write $H(m, n) = \max\{|m|, |n|\}$, thus $|G(m, n)| = |\sum_{i=0}^{D+2-d} g_i m^i n^{D+2-d-i}| \ll$

H^{D+2-d} . Note that for every fixed real α , $|m - \alpha n| \ll H$. Moreover, for every real α and β with $\alpha \neq \beta$ we have $(m - \alpha n) - (m - \beta n) = -(\alpha - \beta)n$, and $\alpha(m - \beta n) - \beta(m - \alpha n) = (\alpha - \beta)m$. Thus, we deduce that $\max\{|m - \alpha n|, |m - \beta n|\} \gg H$. So, since $a(x, y), b(x, y)$ have no common factors, $\max\{|a(m, n)|, |b(m, n)|\} \gg H^D$. Substituting these two estimates into the equation above we get:

$$\prod_{\text{primes } p|F(m,n)} p \gg \frac{\max\{a(m, n), b(m, n)\}^{1-\varepsilon/D}}{G(m, n)} \gg \max\{|m|, |n|\}^{\deg(F)-2-\varepsilon}.$$

□

If we wish to consider $f(X) \in \mathbb{Z}[X]$, then we can obtain a stronger consequence of Theorem 2.1 than comes from simply setting $n = 1$. If $f(X)$ has degree d then we let $F(X, Y) = Y^{d+1}f(X/Y)$; thus $f(X) = F(X, 1)$, but $\deg(F) = \deg(f) + 1$. So now, applying Theorem 2.1,

$$\prod_{\text{primes } p|f(m)} p = \prod_{\text{primes } p|F(m,1)} p \gg \max\{|m|, |1|\}^{\deg(F)-2-\varepsilon} = |m|^{\deg(f)-1-\varepsilon}.$$

This yields

Corollary 2.9. *Assume that the abc-conjecture is true. Suppose that $f(X) \in \mathbb{Z}[X]$, has no repeated roots. Fix $\varepsilon > 0$. Then*

$$\prod_{\text{primes } p|f(m)} p \gg |m|^{\deg(f)-1-\varepsilon}.$$

Where the constant implied by \gg depends on f and ε .

The next result, although an immediate corollary of the Theorem 2.1, will be stated like a Theorem because it will play an important role in what follows.

Theorem 2.10. *Let k be an integer ≥ 2 . Assume that the abc-conjecture is true. Suppose that $F(X, Y) \in \mathbb{Z}[X, Y]$ is homogeneous, without any repeated linear factors. Fix $\varepsilon > 0$. If there exists an integer q such that q^k divides $F(m, n)$ for some coprime integers m and n then $q \ll \max\{|m|, |n|\}^{(2+\varepsilon)/(k-1)}$. Also, if $f(X) \in \mathbb{Z}[X]$ has no repeated roots and q^k divides $f(m)$, then $q \ll |m|^{(1+\varepsilon)/(k-1)}$.*

Here the constants implied by \ll depend on ε , and F, f respectively.

Proof. By Theorem 2.1 we have

$$\prod_{\text{primes } p|F(m,n)} p \gg \max\{|m|, |n|\}^{\deg(F)-2-\varepsilon}.$$

This is equivalent to

$$\max\{|m|, |n|\}^{2+\varepsilon} \cdot \prod_{\text{primes } p|F(m,n)} p \gg \max\{|m|, |n|\}^{\deg(F)}.$$

This implies that

$$|F(m, n)| \ll \max\{|m|, |n|\}^{2+\varepsilon} \cdot \prod_{\text{primes } p|F(m,n)} p.$$

Since clearly

$$q^{k-1} \prod_{\text{primes } p|F(m,n)} p \ll |F(m, n)|,$$

we obtain

$$q \ll \max\{|m|, |n|\}^{(2+\varepsilon)/(k-1)}$$

as required.

In the case $f(X) \in \mathbb{Z}[X]$ the proof is similar. □

Chapter 3

Asymptotic estimate for the density of integers n for which $f(n)$ is k -free

Let k be an integer ≥ 2 ; let $f(X) \in \mathbb{Q}[X]$ be a polynomial such that $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$ and $\gcd_{n \in \mathbb{Z}} f(n)$ is k -free. Now we will use the previous chapters to derive an asymptotic estimate for the number of positive integers $n \leq N$ such that $f(n)$ is k -free. Further we prove that for every $\varepsilon > 0$ and every sufficiently large z there is an integer $m \in [z, z + z^\varepsilon)$, for which $f(m)$ is k -free. Both results are proved assuming the *abc*-conjecture.

3.1 Asymptotic estimate of integers n for which $f(n)$ is k -free

Let k be an integer ≥ 2 and $f(X)$ a polynomial in $\mathbb{Q}[X]$ of degree d without any repeated roots. We assume that $f(m) \in \mathbb{Z}$ for all $m \in \mathbb{Z}$ and $\gcd_{m \in \mathbb{Z}}(f(m))$ is k -free. Under these conditions, we expect that there are infinitely many integers m for which $f(m)$ is k -free but unconditionally this is far from being established.

The following result is an extension of a result of Granville [14] from square-free values to k -free values of polynomials.

Theorem 3.1. *Assume that the *abc*-conjecture is true. Then, as $N \rightarrow \infty$, there are $\sim c_{f,k}N$ positive integers $n \leq N$ for which $f(n)$ is k -free, with:*

$$c_{f,k} := \prod_{p \text{ prime}} \left(1 - \frac{\omega_{f,k}(p)}{p^k} \right)$$

where, for each prime p , $\omega_{f,k}(p)$ denotes the number of integers a in the range $1 \leq a \leq p^k$ for which $f(a) \equiv 0 \pmod{p^k}$.

We first give a definition.

Definition 3.2. For a polynomial $f(X) \in \mathbb{Q}[X]$, we define $L(f) := \text{lcm}(b, \Delta(bf))$, where b is the smallest positive integer such that $bf(X) \in \mathbb{Z}[X]$.

In the prove of this Theorem we need some auxiliary results.

Lemma 3.3 (Hensel's lemma). Let $f(x)$ be a polynomial with integer coefficients of degree d , and let $a_0 \in \mathbb{Z}$ be such that $f(a_0) \equiv 0 \pmod{p}$, $f'(a_0) \not\equiv 0 \pmod{p}$. Then for every $k \geq 1$ there is precisely one congruence class $a \pmod{p^k}$ such that

$$f(a) \equiv 0 \pmod{p^k}, \quad a \equiv a_0 \pmod{p}.$$

Proof. For this proof see also [20]. □

Remark 3.4. If p does not divide the discriminant of f , and $f(r) \equiv 0 \pmod{p}$, then $f'(r) \not\equiv 0 \pmod{p}$.

Corollary 3.5. Let $f(X) \in \mathbb{Q}[X]$ be a polynomial of degree d , such that $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$ and let p be a prime such that p does not divide $L(f)$. Then:

$$\omega_{f,k}(p) = |\{a \pmod{p^k} : f(a) \equiv 0 \pmod{p^k}\}| \leq d.$$

Proof. Let $f(X) = a_0X^d + a_1X^{d-1} + \dots + a_d$. Let b be as in the Definition 3.2 and let $g(X) = bf(X)$. Then $g(X) = b_0X^d + b_1X^{d-1} + \dots + b_d \in \mathbb{Z}[X]$ with $b_i = ba_i$ ($i = 0, 1, \dots, d$).

Now $f(a) \equiv 0 \pmod{p^k}$ is equivalent to $g(a) \equiv 0 \pmod{p^k}$ since p does not divide b .

The congruence $g(X) \equiv 0 \pmod{p}$ has at most d solutions modulo p (since $g(X) = 0 \pmod{p}$ has at most d zeros in \mathbb{F}_p).

Let $x_1, x_2, \dots, x_r \pmod{p}$ be the solutions to $g(X) \equiv 0 \pmod{p}$.

We have $L(f) = \text{lcm}(b, \Delta(g))$, so by assumption, p does not divide $\Delta(g)$. Further,

$$\Delta(g) = \pm b_0 R(g, g').$$

Now if there is an integer a such that $p|g(a)$, $p|g'(a)$ then $p|R(g, g')$. That is, $p|\Delta(g)$. But this is against our assumption.

So if $g(a) \equiv 0 \pmod{p}$, then $g'(a) \not\equiv 0 \pmod{p}$.

Now let $a \pmod{p^k}$ be a solution to $f(x) \equiv 0 \pmod{p^k}$. Then $g(a) \equiv 0 \pmod{p^k}$, so $g(a) \equiv 0 \pmod{p}$. Hence $a \equiv x_i \pmod{p}$ for some $i \in \{1, 2, \dots, r\}$. But the residue class $a \pmod{p^k}$ such that $g(a) \equiv 0 \pmod{p^k}$ and $a \equiv x_i \pmod{p}$ is unique, by Lemma 3.3. □

In what follows, we assume that $f(X) \in \mathbb{Q}[X]$, $f(m) \in \mathbb{Z}$ for all $m \in \mathbb{Z}$ and $\gcd_{m \in \mathbb{Z}} f(m)$ is k -free.

Proposition 3.6. *Let α be a fixed real number ≥ 1 .*

Then uniformly for $u \geq 0$, the number of integers $n \in (u, u + N]$ for which $f(n)$ is not divisible by the k -th power of a prime $p \leq \alpha N$ is $\sim c_{f,k}N$ as $N \rightarrow \infty$.

Remark 3.7. *By this we mean the following: for every $\varepsilon > 0$ there is $N_0 > 0$ such that for every $N \geq N_0$ and every $u \geq 0$ we have:*

$$|S(u, N) - c_{f,k}N| < \varepsilon N,$$

where $S(u, N)$ is the number of integers $n \in (u, u + N]$ such that $f(n)$ is not divisible by the k -th power of a prime $p \leq \alpha N$.

Proof. Let $z = \frac{1}{k+1} \log N$ and choose N large enough such that $z > L(f)$;

let $M = \prod_{p \leq z} p^k = \exp\left(k \sum_{p \leq z} \log p\right) = e^{k\theta(z)}$. By the prime number theorem

$\theta(z) = z + o(z)$, and so $M = e^{\frac{k}{k+1} \log N(1+o(1))} = N^{\frac{k}{k+1}+o(1)}$ as $N \rightarrow \infty$.

For every prime $p \leq z$ and every number $x \geq 0$, there are $\frac{M}{p^k} \omega_{f,k}(p)$ integers $n \in (x, x + M]$ such that $f(n) \equiv 0 \pmod{p^k}$. Hence there are $M \left(1 - \frac{\omega_{f,k}(p)}{p^k}\right)$ integers $n \in (x, x + M]$ such that $f(n)$ is not divisible by p^k . So, by the Chinese Remainder Theorem, there are exactly $M \prod_{p \leq z} \left(1 - \frac{\omega_{f,k}(p)}{p^k}\right)$ integers n in any interval $(x, x + M]$, for which $f(n)$ is not divisible by the k -th power of a prime $p \leq z$. Thus there are

$$M \left(\frac{N}{M} + O(1)\right) \prod_{p \leq z} \left(1 - \frac{\omega_{f,k}(p)}{p^k}\right) = N \left(1 + O\left(\frac{M}{N}\right)\right) \prod_{p \leq z} \left(1 - \frac{\omega_{f,k}(p)}{p^k}\right)$$

integers $n \in (u, u + N]$ for which $f(n)$ is not divisible by the k -th power of a prime $p \leq z$. Notice that the constant implied by O does not depend on u . Now, if a prime p does not divide $L(f)$ then by Corollary 3.4, $\omega_{f,k}(p) \leq d$. Hence

$$\sum_{p > z} \frac{\omega_{f,k}(p)}{p^k} \leq d \sum_{p > z} \frac{1}{p^k} \leq \sum_{n > z} \frac{1}{n^k} \ll \frac{1}{z^{k-1}}.$$

This yields, that $c_{f,k} / \prod_{p \leq z} \left(1 - \frac{\omega_{f,k}(p)}{p^k}\right) = 1 + O\left(\frac{1}{z^{k-1}}\right)$, and so we have proved that, uniformly in u , there are $\sim c_{f,k}N$, as $N \rightarrow \infty$, integers n in the interval $(u, u + N]$ for which $f(n)$ is not divisible by the k -th power of a prime $p \leq z$.

As we have shown above there are $\omega_{f,k}(p)\{N/p^k + O(1)\}$ integers in the interval $(u, u + N]$ for which $f(n) \equiv 0 \pmod{p^k}$, for any given prime p . If $p > z$ then this number is, by Corollary 3.4, $\leq dN/p^k + O(d)$. Therefore the number of integers $n \in (u, u + N]$ such that there is a prime $p \in (z, \alpha N]$ for which $f(n) \equiv 0 \pmod{p^k}$ is

$$\ll_d \sum_{z < p \leq \alpha N} \left(\frac{N}{p^k} + 1 \right) \ll \frac{N}{z^{k-1}} + \frac{N}{\log N} = o(N).$$

Then the number of integers $n \in (u, u + N]$ such that $f(n)$ is not divisible by the k -th power of a prime $p \leq z$ but $f(n) \equiv 0 \pmod{p^k}$ for some prime $p \in (z, \alpha N]$ is equal to $o(N)$ hence the number of integer $n \in (u, u + N]$ for which $f(n)$ is not divisible by the k -th power of a prime $p \leq \alpha N$ is $\sim c_{f,k}N$ uniformly in u as $N \rightarrow \infty$. \square

We complete the proof of Theorem 3.1 by showing that, for any fixed $\varepsilon > 0$, there are $O(\varepsilon N)$ integers $n \leq N$ for which $f(n)$ is divisible by the square of a prime $> N$. Observe that this result is true for $f(X)$ it is true for all irreducible factors of $f(X)$; thus we will assume that $f(X)$ is irreducible. Hence it is sufficient to prove the following:

Theorem 3.8. *Assume that the abc-conjecture is true. Suppose that $f(X) \in \mathbb{Q}[X]$ is irreducible of degree $d \geq 2$, with $f(n) \in \mathbb{Z}$ for $n \in \mathbb{Z}$. Then for every $\varepsilon > 0$ there are $O(\varepsilon N)$ integers $n \leq N$ such that $f(n)$ is divisible by the square of a prime $p > N$.*

Remark 3.9. *We may assume $d \geq 2$ since the square of any prime $p > N$ is $\gg N^2$ and so, if N is sufficiently large, cannot divide a non-zero value of a linear polynomial.*

Proof. Consider the new polynomial,

$$F(X) = f(X)f(X+1)f(X+2)\cdots f(X+l-1),$$

where l is an integer to be chosen later.

We claim that this polynomial has no repeated factors. Indeed, suppose that $F(X)$ has repeated factors. Then, $f(X+i) = f(X+j)$ for certain integers i, j with $i \neq j$, since f is irreducible. By substituting X for $X+i$ we obtain $f(X) = f(X+n)$ where $n = j-i \neq 0$.

Taking $X = 0, n, 2n, \dots$, etc we obtain $f(n) = f(0)$, $f(2n) = f(n) = f(0)$, $f(3n) = f(0), \dots$, i.e. the polynomial $f(X) - f(0)$ has zeros $0, n, 2n, \dots$. This is impossible since f is not constant.

For every $n < N$, write $n = jl + i$, where $0 \leq i < l$ and $0 \leq j < [N/l]$. Note

that if there exist a prime $q > N$ such that q^2 divides $f(n)$, then $q \prod_{p|f(n)} p \leq |f(n)| \ll N^{\deg(f)}$ hence $\prod_{p|f(n)} p \ll N^{\deg(f)-1}$. Thus if two of the $f(n+i)$ were divisible by squares of primes $> N$, we would have $\prod_{p|F(n)} p \ll N^{\deg(F)-2}$, contradicting Corollary 2.9. This implies that there is at most one number $f(n+i), 0 \leq i < l$, which is divisible by the square of a prime $> N$. Thus, in total there are $O(N/l)$ integers $n \leq N$ such that $f(n)$ is divisible by the square of a prime $> N$. Selecting $l = \lceil 1/\varepsilon \rceil$ the result follows. \square

Remark 3.10. *If $k \geq 3$ Theorem 3.1 follows directly from Proposition 3.6 and Theorem 2.10.*

3.2 On gaps between integers at which a given polynomial assumes k -free values

In this section we investigate the problem of finding an as small as possible function $h = h(z)$ such that for a given polynomial f and for every sufficiently large z , there is an integer $m \in (z, z+h]$ such that $f(m)$ is k -free.

The following result was proved by Granville [14] in the case $f(X) = X$, $k = 2$.

Theorem 3.11. *Let $k \geq 2$. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree $d \geq 1$. Assume again that $f(m) \in \mathbb{Z}$ for $m \in \mathbb{Z}$ and that $\gcd_{m \in \mathbb{Z}} f(m)$ is k -free. If the abc-conjecture is true then for every $\varepsilon > 0$ and for every sufficiently large z there is an integer $m \in (z, z+z^\varepsilon]$ such that $f(m)$ is k -free.*

Proof. Choose c such that $c_{f,k} < 1 - c < 1$, and $l := \lceil 5/c\varepsilon \rceil$. Define $g(X) = f(X+1)f(X+2) \cdots f(X+l)$.

By proposition 3.6, there is z_0 depending only on f, l, k, ε such that for every $z > z_0$, there are $< (1-c)z^\varepsilon$ integers $m \in (z, z+z^\varepsilon]$ such that $f(m)$ is not divisible by the k -th power of a prime $\leq z^\varepsilon$. Suppose that there is no integer $m \in (z, z+z^\varepsilon]$ such that $f(m)$ is k -free, thus there are at least cz^ε integers $m \in (z, z+z^\varepsilon]$ such that $f(m)$ is divisible by p^k for some prime $p > z^\varepsilon$.

Assuming z_0 is sufficiently large, $z \geq z_0$, we claim that there is an integer $m_0 \in (z, z+z^\varepsilon]$ such that at least $\frac{c}{2}$ of the integers $f(m_0+1), f(m_0+2), \dots, f(m_0+l)$ are divisible by the k -th power of a prime $> z^\varepsilon$. Thus $g(m)$ is divisible by the square of an integer $> (z^\varepsilon)^{\frac{cl}{2}}$. Hence $g(m)$ is divisible by the square of an integer $> m^2$ and this last statement contradicts Theorem 2.10. \square

Proof of the claim: Assume z_0 is large enough such that $z_0^\varepsilon > l$. Let a be the largest integer at most z and r the largest integer such that $a + rl \leq z + z^\varepsilon$. Suppose that none of the sets $\{a + 1, \dots, a + l\}$, $\{a + l + 1, \dots, a + 2l\}, \dots, \{a + (r - 1)l + 1, \dots, a + rl\}$ contains more than $(c/2)l$ integers m for which $f(m)$ is divisible by the k -th power of a prime $p > z^\varepsilon$. Then $(z, z + z^\varepsilon]$ contains altogether at most

$$\begin{aligned} \frac{c}{2}rl + l &\leq \frac{c}{2}z^\varepsilon + l \\ &\leq \frac{c}{2}z^\varepsilon + \left\lceil \frac{5}{c\varepsilon} \right\rceil \\ &< cz^\varepsilon \end{aligned}$$

such integers, assuming z is sufficiently large, contradicting our assumption. \square

Chapter 4

The average moments of

$$s_{n+1} - s_n$$

In this chapter we will state the most important result of our thesis.

Let k be an integer and let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree d such that $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$ and $\gcd_{n \in \mathbb{Z}} f(n)$ is k -free.

Let $\{s_n\}_{n=1}^{\infty}$ be the ordered sequence of positive integers m such that $f(m)$ is k -free. Suppose that $k \geq \min(3, d + 1)$.

The following result was proved by Granville [14] in the case $f(X) = X$, $k = 2$.

Theorem 4.1. *Suppose the abc-conjecture is true. Then for every real $A > 0$ there exists a constant $\beta_A > 0$ such that:*

$$\sum_{s_n \leq x} (s_{n+1} - s_n)^A \sim \beta_A x \text{ as } x \rightarrow \infty.$$

We start with a Lemma.

Lemma 4.2. *Assume the abc-conjecture. Let a_1, a_2, \dots, a_l be fixed integers. Then there is a number $\gamma_{\underline{a}} = \gamma_{\{a_1, a_2, \dots, a_l\}}$ such that the number of integers $m \leq x$ such that $f(m), f(m + a_1), \dots, f(m + a_l)$ are all k -free is $\sim \gamma_{\underline{a}} x$ as $x \rightarrow \infty$.*

Proof. As we have seen in the proof of Theorem 3.8, since f is irreducible, no two among the polynomial $f(X), f(X + a_1), \dots, f(X + a_l)$ have a common factor. So for $i, j \in \{1, 2, \dots, l\}$ with $i \neq j$, the resultant $R_{i,j}$ of $f(X + a_i)$ and $f(X + a_j)$ is $\neq 0$. Let $y = \max\{|R_{i,j}| : 1 \leq i, j \leq l, i \neq j\}$, then if p is a prime with $p > y$ then p divides at most one of the polynomials $f(m), f(m + a_1), \dots, f(m + a_l)$.

Now let $M = \left(\prod_{p \leq y} p \right)^k$, and let \mathcal{A} be the set of integers $a \in [0, M - 1)$ such that none of $f(a), f(a + a_1), \dots, f(a + a_l)$ is divisible by the k -th power of a prime $p \leq y$. Hence for every integer m with $0 \leq m \leq x$ we have: $f(m), f(m + a_1), \dots, f(m + a_l)$ all k -free is equivalent to $m = a \pmod{M}$ for some $a \in \mathcal{A}$ and $f(m), f(m + a_1), \dots, f(m + a_l)$ not divisible by p^k for some prime $p > y$.

Writing $m = m'M + a$ with $a \in \mathcal{A}$ we obtain:

$f(m), f(m + a_1), \dots, f(m + a_l)$ k -free is equivalent to $m = a \pmod{M}$ for some $a \in \mathcal{A}$ and $g_a(m')$ k -free, where $g_a(X) = f(a + MX)f(a_1 + a + MX) \dots f(a_l + a + MX)$.

Now according to Theorem 3.1 assuming the *abc*-conjecture, there is $c_a \geq 0$ such that

$$\#\{m' \leq x' : g_a(m') \text{ is } k\text{-free}\} \sim c_a x' \quad \text{as } x' \rightarrow \infty.$$

So

$$\begin{aligned} |\{m \leq x : f(m), f(m + a_1), \dots, \\ f(m + a_l), \text{ are } k\text{-free}\}| &= \sum_{a \in \mathcal{A}} \#\left\{m' \leq \frac{x - a}{M} : g_a(m') \text{ } k\text{-free}\right\} \\ &\sim \left(\sum_{a \in \mathcal{A}} \frac{c_a}{M}\right) x \quad \text{as } x \rightarrow \infty. \end{aligned}$$

□

Proof of Theorem 4.1. We introduce some new definitions to simplify our proof:

First, let $S(x; t)$ be the number of integers n such that $s_n \leq x$ and $s_{n+1} - s_n = t$.

Let $S'(x, T)$ denote the number of integers n such that $s_n \leq x$, and $T \leq s_{n+1} - s_n < 2T$, and such that there are $\geq (5c/6)T$ integers m in the interval (s_n, s_{n+1}) such that $f(m)$ is not divisible by the k -th power of a prime $\leq 2T$ or $> T^A$.

Let t be a positive integer. For any subset I of $\{1, 2, \dots, t - 1\}$ we denote by S_I the set of integers $n \leq x$ for which $f(n), f(n + t)$ and $f(n + a)$ for all $a \in I$ are k -free. Notice that $|S_\emptyset|$ denotes the number of integers $n \leq x$ such that $f(n), f(n + t)$ are k -free and without conditions for $f(n + 1), f(n + 2), \dots, f(n + t - 1)$. Then by Lemma 4.2, we have $|S_I| \sim \gamma_{I \cup \{0,1\}} x$ for some

$\gamma_{I \cup \{0,1\}} > 0$ and by the rule of inclusion-exclusion,

$$\begin{aligned} S(x, t) &= |S_\emptyset| - \sum_{i=1}^{t-1} |S_{\{i\}}| + \sum_{1 \leq i_1 < i_2 \leq t-1} |S_{\{i_1, i_2\}}| - \sum_{1 \leq i_1 < i_2 < i_3 \leq t-1} |S_{\{i_1, i_2, i_3\}}| + \dots \\ &= \sum_I (-1)^{|I|} S_I \sim \sum_I (-1)^{|I|} \gamma_{I \cup \{0,1\}} x = \delta_t x \end{aligned}$$

as $x \rightarrow \infty$.

We claim, that under assumption of the *abc*-conjecture, we have for every sufficiently large x , and $T > 0$,

$$\sum_{T \leq t < 2T} S(x, t) \ll_A x/T^{A+1}.$$

Then we have:

$$\begin{aligned} \frac{1}{x} \sum_{t \geq T} S(x, t) t^A &= \frac{1}{x} \sum_{j=0}^{\infty} \sum_{2^j T \leq t < 2^{j+1} T} S(x, t) t^A \\ &\ll \frac{1}{x} \sum_{j=0}^{\infty} \frac{x}{(2^j T)^{A+1}} (2^{j+1} T)^A \\ &\ll \frac{2^A}{T} \sum_{j=0}^{\infty} \left(\frac{1}{2}\right)^j \\ &\ll \frac{1}{T}. \end{aligned}$$

Therefore

$$\begin{aligned} \frac{1}{x} \sum_{s_n \leq x} (s_{n+1} - s_n)^A &= \frac{1}{x} \sum_{t=1}^{\infty} S(x, t) t^A \\ &= \frac{1}{x} \sum_{t=1}^T S(x, t) t^A + \frac{1}{x} \sum_{t \geq T} S(x, t) t^A \\ &= \frac{1}{x} \sum_{t=1}^T S(x, t) t^A + E(x, T), \text{ with } |E(x, T)| \leq \frac{c_1}{T}, \end{aligned}$$

where c_1 is independent of x .

Fixing T and letting $x \rightarrow \infty$, we infer, $\frac{1}{x} \sum_{t=1}^T S(x, t) t^A \rightarrow \sum_{t=1}^T \delta_t t^A$.

Hence $\frac{1}{x} \sum_{t=1}^{\infty} S(x, t) t^A$ is bounded as $x \rightarrow \infty$, by say c_2 .

Now:

$$\frac{1}{x} \sum_{t=1}^T S(x, t)t^A \leq \frac{1}{x} \sum_{t=1}^{\infty} S(x, t)t^A + \frac{c_1}{T} \leq c_2 + \frac{c_1}{T}$$

for all x .

This implies $\sum_{t=1}^T \delta_t t^A \leq c_2 + \frac{c_1}{T}$; so $\sum_{t=1}^T \delta_t t^A$ is bounded independently of T .

Thus $\beta_A := \sum_{t=1}^{\infty} \delta_t t^A$ converges.

Let $\delta > 0$ then for every $T > 0$ there is $x_0(\delta, T)$ such that

$$\left| \frac{1}{x} \sum_{t=1}^T S(x, t)t^A - \sum_{t=1}^T \delta_t t^A \right| < \frac{\delta}{3}$$

for all $x \geq x_0(\delta, T)$. There is T_0 such that

$$\left| \sum_{t=1}^T \delta_t t^A - \beta_A \right| < \frac{\delta}{3}$$

for all $T \geq T_0$.

Take $T \geq \max(T_0, \frac{c_2}{3\delta})$ and then $x \geq x_0(\delta, T)$, thus,

$$\begin{aligned} \left| \frac{1}{x} \sum_{s_n \leq x} (s_{n+1} - s_n)^A - \beta_A \right| &= \left| \frac{1}{x} \sum_{t=1}^{\infty} S(x, t)t^A - \beta_A \right| \\ &\leq \left| \frac{1}{x} \sum_{t=1}^{\infty} S(x, t)t^A - \frac{1}{x} \sum_{t=1}^T S(x, t)t^A \right| \\ &\quad + \left| \frac{1}{x} \sum_{t=1}^T S(x, t)t^A - \sum_{t=1}^T \delta_t t^A \right| + \left| \sum_{t=1}^T \delta_t t^A - \beta_A \right| \\ &\leq \frac{c_1}{T} + \frac{\delta}{3} + \frac{\delta}{3} \\ &\leq \frac{\delta}{3} + \frac{\delta}{3} + \frac{\delta}{3} = \delta. \end{aligned}$$

So $\frac{1}{x} \sum_{n \leq x} (s_{n+1} - s_n)^A \rightarrow \beta_A$ as $x \rightarrow \infty$. □

We can assume that T is sufficiently large. By Theorem 3.11, we know that $S(x, t) = 0$ when $t \geq x^\varepsilon$ and x is sufficiently large. We apply this with

$$\varepsilon = \begin{cases} \min\left(\frac{1}{kA(A+1)}, \frac{k-5/2}{A(k-1)^2}\right) & \text{if } k \geq 3, d \geq 2, \\ \frac{1}{kA(A+1)} & \text{if } k \geq 2, d = 1. \end{cases}$$

Thus we will prove the claim assuming that $T < x^\varepsilon$ and x is sufficiently large. Let B be the smallest integer $\geq A$.

Proof of the claim: By Proposition 3.6, there are $\geq ct$ integers m , for some constant $c < c_{f,k}$, in any interval of length $t \geq T$, for which $f(m)$ is not divisible by the k -th power of a prime $\leq 2T$. For any $s_n \leq x$ counted by $\sum_{T \leq t < 2T} S(x; t)$ but not by $S'(x, T)$, there must be $> (c/6)T$ integers $m \in (s_n, s_{n+1})$ for which $f(m)$ is divisible by the k -th power of a prime $p > T^A$. Otherwise there would be at most $(c/6)T$ integers $m \in (s_n, s_{n+1})$ for which $f(m)$ is divisible by the k -th power of a prime $p > T^A$, implying that we have $\geq T - (c/6)T > (5c/6)T$ integers $m \in (s_n, s_{n+1})$ for which $f(m)$ is not divisible by the k -th power of a prime $p > T^A$. But this means precisely that $s_n \in S'(x, T)$, contradicting our choice. Therefore

$$\begin{aligned}
\frac{cT}{6} \left(\sum_{T \leq t < 2T} S(x, t) - S'(x, T) \right) &\leq \sum_{\substack{m \leq x \\ \exists p > T^A: p^k | f(m)}} 1 \\
&\leq \sum_{p > T^A} \sum_{\substack{m \leq x, \\ p^k | f(m)}} 1 \\
&\leq \sum_{p > T^A} \omega_{f,k}(p) \left(\frac{x}{p^k} + 1 \right) \\
&\ll_d \sum_{p > T^A} \frac{x}{p^k} + \sum_{\substack{p > T^A \\ \exists m \leq x: p^k | f(m)}} 1 \\
&\ll_d \frac{x}{T^{A(k-1)}} + \sum_{\substack{p > T^A \\ \exists m \leq x: p^k | f(m)}} 1.
\end{aligned}$$

We show that the last sum is $\ll \frac{x}{T^{A(k-1)}}$. First assume that $k \geq 2, d = 1$. Then if $p^k | f(m)$ we have $p \ll |m|^{1/k} \ll x^{1/k}$ hence

$$\sum_{\substack{p > T^A \\ \exists m \leq x: p^k | f(m)}} 1 \ll x^{1/k} \ll \frac{x}{T^{A(k-1)}}$$

by our assumption $T < x^{\frac{1}{kA(A+1)}}$.

Second assume that $k \geq 3, d \geq 2$. If $p^k | f(m)$ for some integer $m \leq x$,

by Theorem 2.10, $p \ll_{\theta} |m|^{\frac{1+\theta}{k-1}} \ll x^{\frac{1+\theta}{k-1}}$, for every $\theta > 0$, so in particular $p \leq x^{\frac{3/2}{k-1}}$ if x is sufficiently large. Hence

$$\sum_{\substack{p > T^A \\ \exists m \leq x: p^k | f(m)}} 1 < x^{\frac{3/2}{k-1}} < \frac{x}{T^{A(k-1)}},$$

by our assumption $T < x^{\frac{k-5/2}{A(k-1)^2}}$. Thus we conclude that if x is sufficiently large and $T < x^{\varepsilon}$ we have

$$\left(\sum_{T \leq t < 2T} S(x, t) - S'(x, T) \right) \ll \frac{x}{T^{A(k-1)+1}} \ll \frac{x}{T^{A+1}}.$$

For every s_n counted by $S'(x; T)$ we have $\geq (5c/6)T$ integers in the interval (s_n, s_{n+1}) such that $f(m)$ is divisible by the k -th power of a prime in the range $[2T, T^A]$. We consider B -tuples of such integers

$$s_n < m_1 < m_2 < \dots < m_B < s_{n+1}.$$

For such a tuple there are primes p_1, p_2, \dots, p_B with $2T \leq p_i < T^A$ for $i \in \{1, 2, \dots, B\}$ such that

$$f(m_j) \equiv 0 \pmod{p_j^k},$$

and the number of such integers is at least $\binom{\lfloor (5c/6)T \rfloor}{B}$.

Let $i_1 = 1, q_1 = p_1$; let i_2 be the smallest index $i \in \{2, 3, \dots, B\}$ such that $p_i \neq p_1$ put $q_2 = p_{i_2}$; let i_3 be the smallest index $i \in \{3, 4, \dots, B\}$ such that $p_{i_3} \notin \{q_1, q_2\}$; put $q_3 = p_{i_3}$, etc. Consider this sequence, $i_1 = 1 < i_2 < \dots < i_u \leq B$ of indices. Let $d_2 = m_{i_2} - m_1, d_3 = m_{i_3} - m_1, \dots, d_u = m_{i_u} - m_1$.

The number of possibilities for (d_2, d_3, \dots, d_u) is

$$\leq (2T)^{u-1}.$$

Now for any fixed (d_2, d_3, \dots, d_u) we have

$$\left\{ \begin{array}{l} f(m_1) \equiv 0 \pmod{q_1^k} \\ f(m_{i_2}) \equiv 0 \pmod{q_2^k} \\ f(m_{i_3}) \equiv 0 \pmod{q_3^k} \\ \vdots \\ f(m_{i_u}) \equiv 0 \pmod{q_u^k} \end{array} \right\} \iff \left\{ \begin{array}{l} f(m_1) \equiv 0 \pmod{q_1^k} \\ f(m_1 + d_2) \equiv 0 \pmod{q_2^k} \\ f(m_1 + d_3) \equiv 0 \pmod{q_3^k} \\ \vdots \\ f(m_1 + d_u) \equiv 0 \pmod{q_u^k} \end{array} \right.$$

By Corollary 3.4, m_j is congruent to one of $\leq d$ incongruent numbers modulo q_j^k for each j . So by the Chinese Remainder Theorem, m_1 belong to one of at most d^u residue classes modulo $(q_1q_2 \dots q_u)^k$. Hence for each of these residue classes we have

$$d^u \left(x / (q_1q_2 \dots q_u)^k + 1 \right)$$

possibilities for m_1 ; since $(q_1q_2 \dots q_u)^k \leq T^{Auk} \leq T^{ABk} \leq T^{A(A+1)k} < x$ this gives at most

$$\frac{2x}{(q_1q_2 \dots q_u)^k} d^u$$

possibilities for m_1 .

Taking into account the possibilities for (d_2, d_3, \dots, d_u) we get at most

$$\ll T^{u-1} \left(x / (q_1q_2 \dots q_u)^k \right)$$

possibilities for $(m_1, m_{i_2}, \dots, m_{i_u})$.

It remains to take into account the m_i with $i \notin \{1, i_2, \dots, i_u\}$.

Let $i \notin \{1, i_2, i_3, \dots, i_u\}$. Then $p_i = q_j$ for some $j \in \{1, 2, \dots, u\}$, hence

$$f(m_i) \equiv f(m_{i_j}) \equiv 0 \pmod{q_j^k}.$$

Let $\omega_1, \omega_2, \dots, \omega_r$ be the solutions of $f(x) \equiv 0 \pmod{q_j}$, $0 \leq x < q_j$. Then by corollary 3.4, $r \leq \deg(f)$. Now since $|m_{i_j} - m_i| \leq 2T < q_j$ we have $m_{i_j} - m_i = \omega_{l_1} - \omega_{l_2}$ for some $l_1, l_2 \in \{1, 2, \dots, r\}$. So given m_{i_j} , there are at most d^2 possibilities for m_i .

This gives altogether at most

$$(d^2)^{B-u}$$

possibilities for the tuples $(m_i : i \notin \{1, i_2, i_3, \dots, i_u\})$.

Hence for the tuples (m_1, m_2, \dots, m_B) we have at most

$$T^{u-1} \left(x / (q_1q_2 \dots q_u)^k \right) (2d^2)^{B-u} \ll T^{u-1} \left(x / (q_1q_2 \dots q_u)^k \right)$$

possibilities where q_1, q_2, \dots, q_u are the distinct primes among p_1, p_2, \dots, p_B . For given q_1, q_2, \dots, q_u there are at most $u^B \leq B^B \ll 1$ possi-

bilities for p_1, p_2, \dots, p_B so:

$$\begin{aligned}
S'(x, T)T^B &\ll \sum_{u=1}^B \sum_{2T < q_1 < \dots < q_u < T^A} T^{u-1} \frac{x}{(q_1 \dots q_u)^k} \\
&\ll x \sum_{u=1}^B T^{u-1} \left(\sum_{q > 2T} \frac{1}{q^k} \right)^u \\
&\ll x \sum_{u=1}^B T^{u-1} \left(\frac{1}{T^{k-1}} \right)^u \\
&\ll \frac{x}{T}
\end{aligned}$$

Hence

$$S'(x, T) \ll \frac{x}{T^{B+1}} \ll \frac{x}{T^{A+1}},$$

which proves our claim, and completes the proof of Theorem 4.1. □

Bibliography

- [1] B. Beasley, M. Filaseta, *A Distribution Problem for Power Free Values Of Irreducible Polynomials*, *Periodica Mathematica Hungarica* Vol. 42 (1 – 2), 2001, pp. 123 – 144.
- [2] G.V. Belyi, *On the Galois extensions of the maximal cyclotomic field (in Russian)*, *Izv. Akad. Nauk SSSR*. **43**, (1979), 267 – 276
- [3] J. Browkin, M. Filaseta, G. Greaves and A. Schinzel, *Squarefree values of polynomials and the abc-conjecture*, *Sieve Methods, Exponential Sums, and their Applications in Number Theory*, Cambridge U.Press, 1997, pp. 65 – 85.
- [4] N. Elkies, *ABC implies Mordell*, *Int. Math Res. Not.* **7**(1991), 99 – 109.
- [5] P. Erdős, *Some problems and results in elementary number theory*, *Publ. Math. Debrecen* **2** (1951), 103 – 109.
- [6] P. Erdős, *Arithmetical Properties of Polynomials*, *J. London Math. Soc.* **28** (1953), 416 – 425.
- [7] P. Erdős, *Problems and results on consecutive integers*, *Publ. Math. Debrecen* **23** (1976), 271 – 282.
- [8] M. Filaseta, *On the distribution of gaps between squarefree numbers*, *Mathematika* **40** (1993), 88 – 101.
- [9] M. Filaseta, *Short interval results for k -free values of irreducible polynomials*, *Acta Arith.* **64** (1993), 249 – 270.
- [10] M. Filaseta and O. Trifonov, *On gaps between squarefree numbers*, *Progress in Mathematics* **85** (1990), 235 – 253.
- [11] M. Filaseta and O. Trifonov, *On gaps between squarefree numbers II*, *London Math. Soc.* **45** (1992), 215 – 221.

- [12] *M. Filaseta and O. Trifonov, The distribution of fractional parts with applications to gap results in number theory, Proc. London Math. Soc.* **73** (1996), 241 – 278.
- [13] *S. W. Graham, Moments of gaps between k -free numbers, Journal of Number Theory* **44** (1993), 105 – 117.
- [14] *A. Granville, ABC Allows us to count squarefrees, Int. Math. Res. Not.* **19** (1998) 991 – 1009.
- [15] *A. Granville, On the scarcity of powerful binomial coefficients, Matematika,* **46** (1999) 397 – 410.
- [16] *A. Granville, It's as easy as abc, Amer. Math. Soc.* 49 (2002), no. 10, 1224 – 1231.
- [17] *G. Greaves, Power-free values of binary forms, Quart. J. Math. Oxford* **43** (1992), 45 – 65.
- [18] *C. Hooley, On the power free values of polynomials, Mathematica* **14** (1997), 21 – 26.
- [19] *C. Hooley, On the distribution of square free numbers, Can. J. Math.* **25** (1973), 1216 – 1223.
- [20] *N. Koblitz, p -adic Numbers, p -adic Analysis, and Zeta-Functions Springer Verlag,*
- [21] *S. Lang, Algebra, Springer Verlag, Third Edition (2005)*
- [22] *M. Langevin, Cas d'egalite pour le theoreme de Mason et applications de la conjecture (abc), C. R. Acad. Sci. Paris* **317** (1993), 441 – 444.
- [23] *M. Langevin, Partie sans facteur carre de $F(a,b)$ (modulo la conjecture (abc)), Seminaire de Theorie des nombres, Publ. Math. Univ. Caen (1993 – 94).*
- [24] *R. Miranda, Algebraic Curves and Riemann Surfaces, American Mathematical Society (1995).*
- [25] *J. Neukirch, Algebraische Zahlentheorie, Springer Verlag, (1992) .*
- [26] *K. F. Roth, On the gaps between squarefree numbers , J. London. Math. Soc.(2)* **26** (1951), 263 – 268.

- [27] J. -P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, *Invent. Math.* **15** (1972), 259 – 331.
- [28] J. -P. Serre, *Lectures on the Mordell-Weil Theorem*, Vieweg, Braunschweig, (1990).
- [29] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer Verlag (1986).
- [30] P. Vojta, *Diophantine Approximations and Value Distribution Theory*, *Lecture Notes in Math.* **1239** (1987).