THE ABC CONJECTURE, ARITHMETIC PROGRESSIONS OF PRIMES AND SQUAREFREE VALUES OF POLYNOMIALS AT PRIME ARGUMENTS

HECTOR PASTEN

Abstract. On the ABC conjecture, we get an asymptotic estimate for the number of squarefree values of a polynomial at prime arguments. A key tool in our argument is a result by Tao and Ziegler (improving a previous result by Green and Tao) concerning arithmetic progressions of primes.

1. Introduction

Let $r \geq 2$ and let $f \in \mathbb{Z}[t]$ be a polynomial of degree r. In this paper p, q always denote primes. Define

$$N_f(x) = \#\{p \leq x : f(p) \text{ is squarefree}\}$$

Define $\rho_f(n)$ as the number of solutions $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ of the congruence $f(x) \equiv 0 \mod n$.

It is natural to expect that if f has no repeated factor in $\mathbb{Z}[t]$, then f takes infinitely many squarefree values at prime arguments unless there is a local obstruction for this to happen. A simple probabilistic heuristic leads to a conjectural asymptotic formula for $N_f(x)$: taking $n \in [1, x]$ at random we expect that n is prime with probability $1/\log x$. Provided that n is prime, for any given prime p we expect that p^2 divides $f(n)$ with probability $\rho_f(p^2)/\phi(p^2)$ where ϕ is Euler's function, and hence, we expect that $f(n)$ is squarefree (provided that n is prime) with probability

$$c_f = \prod_p \left(1 - \frac{\rho_f(p^2)}{\phi(p^2)}\right).$$

Therefore, this heuristic suggests that $N_f(x)/x \approx c_f/\log x$ and one can conjecture that if f has no repeated factor then

$$N_f(x) = c_f \frac{x}{\log x} + o\left(\frac{x}{\log x}\right). \tag{1}$$

It turns out that the formula (1) is known unconditionally when f has degree $r \leq 3$, see [5] and the references therein. However, it is remarkable that already the case of degree 3 requires highly non-trivial results, such as the modularity theorem of Wiles *et al.*

To the best of our knowledge, there is no known example of an irreducible polynomial f of degree bigger than 3 for which the asymptotic formula (1) is proved.

On the other hand, in [8] it is shown that the ABC conjecture implies a similar asymptotic formula for counting a-th power free values of polynomials at primes, for any fixed $a \geq 3$. The case $a = 2$ (i.e. squarefree values) was also studied in [8] but the ABC conjecture alone was not enough, and it was also necessary to assume the GRH and the so-called *abscissa conjecture*, the latter being a rather strong hypothesis for which not much evidence is known. Note that they also obtain an error term under these assumptions, but they comment that it is not clear if the ABC conjecture alone can give an asymptotic formula. See Theorem 16 in [8] and the discussion after it.

In this note we prove that the ABC conjecture for number fields implies the asymptotic formula (1). More precisely, we prove:

Date: August 3, 2014.

2010 *Mathematics Subject Classification.* Primary 11N32; Secondary 11N13, 11J97, 11N36.

Key words and phrases. Squarefree, primes, polynomial, ABC conjecture, arithmetic progressions of primes.

Partially supported by an Ontario Graduate Scholarship (at Queen's University) and a Benjamin Peirce Fellowship (at Harvard University).

Theorem 1.1. *Let $f \in \mathbb{Z}[t]$ be a polynomial without repeated factors in $\mathbb{Z}[t]$. Assume that the ABC conjecture for number fields holds for each number field $\mathbb{Q}(\alpha)$ where α varies over the irrational roots of f. Then*

$$N_f(x) \sim c_f \frac{x}{\log x}$$

where

$$c_f = \prod_p \left(1 - \frac{\rho_f(p^2)}{p(p-1)}\right).$$

The infinite product defining c_f converges absolutely to a non-zero constant if and only if each individual factor is non-zero. Using Hensel's lemma one can bound $\rho_f(p^2)$ by an effective constant (see Lemma 2.2 below), hence:

Corollary 1.2. *Let f be polynomial with integer coefficients without repeated factors. Assume that the ABC conjecture for number fields holds for each number field $\mathbb{Q}(\alpha)$ where α varies over the irrational roots of f. There is a computable constant $B = B(f)$ such that the following are equivalent:*

- *f takes squarefree values at infinitely many primes.*
- *f takes squarefree values at each prime in a set of positive density among primes.*
- *For each prime $p < B$ one has $\rho_f(p^2) < p(p-1)$.*

The proof of Theorem 1.1 involves a new approach to the problem of counting squarefree values of polynomials, which is mainly based in two new ingredients. The first one corresponds to an application of the ABC conjecture in a way which is 'dual' to previous applications in the problem of counting squarefree values. Roughly speaking, we do not vary the argument n of $f(n)$ to apply the ABC conjecture, but we fix the arguments and vary the polynomial, see Theorem 4.2 below and the discussion in Section 4. The second one is an application of recent results of Tao and Ziegler [11] (extending previous work by Green and Tao [4]) about arithmetic progressions of primes.

In a nutshell, the proof goes as follows: a standard sieve argument gives the desired asymptotic formula up to some extra terms. The most problematic term is the cardinal of $P \cap [1, x]$ for certain set of primes P. We use the ABC conjecture to prove that for a suitable fixed M (indeed, $M = 6(\deg f)^3 + 1$ will suffice) the set P has no arithmetic progressions of length M (with certain additional hypothesis), and then the results of Green, Tao and Ziegler show that P must have density zero. Hence $\#P \cap [1, x]$ only contributes to the error term.

We remark that our sieve methods are standard for this type of problems (see for instance Section 9 in [8] or Section 2 in [5] for similar reductions), although the details in Section 2 below have been worked out focusing on our present goal. On the other hand, our new contributions to the problem are (as explained above) the 'dual' way to apply the ABC conjecture, and the use of results on long arithmetic progressions of primes to control error terms. These two ingredients are what allow us to show that the problem of counting squarefree values at prime arguments is indeed within the range of applications of the ABC conjecture (which was not clear, as discussed in [8]).

Since several generalizations of the ABC conjecture are stated in the literature, it may be useful to conclude this introduction by stating the precise version that we will need (see Section 4 for the precise definition of the *truncated counting function* $N^{(1)}_{K,S}$ and the *height* h_K).

Conjecture 1.3 (ABC for number fields)**.** *Let K be a number field. Let $\epsilon > 0$ and fix mutually distinct elements $b_1, \dots, b_M \in K$. Let S be a finite set of places of K. Then for all but finitely many $\alpha \in K$ one has*

$$(M - 2 - \epsilon) h_K(\alpha) < \sum_{i=1}^{M} N^{(1)}_{K,S}(\alpha - b_i).$$

See Remark 14.4.17 in p. 497 [1] for a more detailed discussion (note that the version with $M = 3$ implies the general case, and when $K = \mathbb{Q}$ this is nothing but the classical ABC conjecture of Masser and Oesterlé). In particular, this is weaker than Vojta's ABC conjecture for algebraic numbers of bounded degree [13] (we only consider one number field at time), which in turn is weaker than the uniform ABC conjecture for algebraic numbers (see for instance [3] for a statement of the latter). For the sake of completeness, in Section 7 we give a related application of Vojta's ABC conjecture for

algebraic numbers of bounded degree which can be useful in other problems, but is not needed for proving Theorem 1.1.

2. Sieving

In this section we perform some standard sieve computations to show that, in order to prove Theorem 1.1 it suffices to prove:

Theorem 2.1. *Let f be as in Theorem 1.1. Assume that the ABC conjecture for number fields holds for each number field $\mathbb{Q}(\alpha)$ where α varies over the irrational roots of f. Given $\epsilon > 0$, define*

$$\Sigma_x = \{p \leq x : \exists q > x^{1-\epsilon}, q^2 | f(p)\}.$$

Then there is a choice of $\epsilon = \epsilon_0 > 0$ depending only on f, for which

$$\#\Sigma_x = o\left(\frac{x}{\log x}\right).$$

In the rest of this section, x is a variable that grows to infinity and $\epsilon > 0$ is a *fixed* parameter smaller than a constant. Let $y = (\log x)/8$ and $z = x^{1-\epsilon}$, and note that both quantities grow with x (and depend on ϵ). We will use the variables ε and τ to denote positive quantities, as small as needed at different points of our arguments in this section.

Consider the sets

$$Q = \{p \leq x : \forall q \leq y, q^2 \nmid f(p)\}$$
$$R = \{p \leq x : \exists q \in (y, z], q^2 | f(p)\}$$
$$S = \{p \leq x : \exists q > z, q^2 | f(p)\}.$$

Note that $S = \Sigma_x$ in the notation of Theorem 2.1, and note also that

$$\#Q \geq N_f(x) \geq \#Q - \#R - \#S. \tag{2}$$

As usual, write $\pi(x)$ for the number of primes $p \leq x$, and write $\pi(x; m, b)$ for the number of primes $p \leq x$ with $p \equiv b(m)$.

If X is a statement, we define $\delta(X) = 1$ if X is true, and $\delta(X) = 0$ if X is false. Define $Y = \prod_{q \leq y} q$ and note that $Y \leq x^{1/4}$ because $\pi(y) \leq 2y/\log y$ and $y = (\log x)/8$.

The next lemma is a standard application of Hensel's lemma, and it is a key ingredient in our estimates.

Lemma 2.2. *For every $\varepsilon > 0$ the inequality $\rho_f(n) < n^\varepsilon$ holds for all $n \gg_\varepsilon 1$.*

Proof. By Hensel's lemma, one can show that there is a constant C such that for all prime powers p^r one has $\rho_f(p^r) < C$. Indeed, $\rho_f(p^r)$ is bounded by the total number of roots of f in $\mathbb{Z}/p^r\mathbb{Z}$, and the latter quantity is absolutely (and effectively) bounded by a constant that only depends on f (this is standard; see for instance Lemma 5.2 in [9]).

Since ρ_f is multiplicative and bounded on prime powers, the result follows. □

Lemma 2.3. *For any given $\tau > 0$ we have*

$$\sum_{y < d \leq x^{1/2-\tau}} \sum_{\substack{a \in (\mathbb{Z}/d^2\mathbb{Z})^\times \\ f(a) \equiv 0 (d^2)}} \pi(x; d^2, a) = o\left(\frac{x}{\log x}\right).$$

Proof. The Brun-Titchmarsh theorem gives

$$\sum_{y < d \leq x^{1/2-\tau}} \sum_{\substack{a \in (\mathbb{Z}/d^2\mathbb{Z})^\times \\ f(a) \equiv 0 (d^2)}} \pi(x; d^2, a) \ll \sum_{y < d \leq x^{1/2-\tau}} \rho_f(d^2) \frac{x}{\phi(d^2)\log(x/d^2)} \leq \frac{x}{\log(x^{2\tau})} \sum_{d > y} \frac{d^\varepsilon}{d^{2-\varepsilon}} = o\left(\frac{x}{\log x}\right)$$

where we used $\rho_f(n) \ll n^\varepsilon$ and $\phi(n) \gg n/\log\log n$, and ε can be taken equal to $1/4$, say. □

Lemma 2.4. *We have*

$$\prod_{q\leq y}\left(1-\frac{\rho_f(q^2)}{\phi(q^2)}\right)=c_f+o(1)$$

with c_f as in Theorem 1.1.

Proof. Let P be the product in question. If $c_f=0$ then $P=0$ for some y large enough, since $\rho_f(q^2)/\phi_f(q^2)\ll q^{-2+\varepsilon}$. On the other hand, if $c_f\neq 0$ then

$$1<P/c_f=\prod_{q>y}\left(1-\frac{\rho_f(q^2)}{\phi_f(q^2)}\right)^{-1}<\prod_{q>y}\left(1-\frac{1}{q^{2-\varepsilon}}\right)^{-1}<1+\sum_{n>y}\frac{1}{n^{2-\varepsilon}}=1+o(1).$$

In any case, $P=c_f+o(1)$. □

Lemma 2.5. *We have*

$$\#Q=c_f\pi(x)+o(\pi(x)).$$

Proof. Observe that

$$\begin{aligned}\#Q&=\sum_{p\leq x}\prod_{q\leq y}(1-\delta(q^2|f(p)))=\sum_{p\leq x}\sum_{d|Y}\mu(d)\delta(d^2|f(p))\\&=\sum_{d|Y}\mu(d)\sum_{p\leq x}\delta(d^2|f(p))\\&=\sum_{d|Y}\mu(d)\sum_{a\in(\mathbb{Z}/d^2\mathbb{Z})^\times}\sum_{\substack{p\leq x\\ p\equiv a(d^2)}}\delta(d^2|f(p))+\sum_{d|Y}\mu(d)O\left(\omega(d)\right)\\&=\sum_{d|Y}\mu(d)\sum_{\substack{a\in(\mathbb{Z}/d^2\mathbb{Z})^\times\\ f(a)\equiv 0(d^2)}}\pi(x;d^2,a)+O(2^{\omega(Y)}).\end{aligned}$$

Note that $2^{\omega(Y)}\leq Y\leq x^{1/4}$ hence

$$\#Q=\sum_{d|Y}\mu(d)\sum_{\substack{a\in(\mathbb{Z}/d^2\mathbb{Z})^\times\\ f(a)\equiv 0(d^2)}}\pi(x;d^2,a)+o\left(\frac{x}{\log x}\right).$$

Write this sum as $U+V$ where U runs over $d\leq y$ with $d|Y$, and V over $d>y$ with $d|Y$. Note that in V we have $d\leq Y\leq x^{1/4}$, hence, Lemma 2.3 gives

$$|V|=o\left(\frac{x}{\log x}\right).$$

Let U' be the sum obtained if in U we substitute $\pi(x;d^2,a)$ by $\pi(x)/\phi(d^2)$. Since $y\ll\log x$ we can use the Siegel-Walfisz theorem to get

$$\begin{aligned}|U-U'|&\leq\sum_{\substack{d\leq y\\ d|Y}}\sum_{\substack{a\in(\mathbb{Z}/d^2\mathbb{Z})^\times\\ f(a)\equiv 0(d^2)}}\left|\pi(x;d^2,a)-\frac{\pi(x)}{\phi(d^2)}\right|\\&\ll y\left(\max_{d\leq y}\rho_f(d^2)\right)\frac{x}{(\log x)^4}\\&\ll\frac{xy^{1+\varepsilon}}{(\log x)^4}.\end{aligned}$$

As $y\ll\log x$, we can take $\varepsilon=1$ to find $|U-U'|=o(x/\log x)$. Therefore

$$Q=U'+o\left(\frac{x}{\log x}\right)=\pi(x)\sum_{\substack{d\leq y\\ d|Y}}\mu(d)\frac{\rho_f(d^2)}{\phi(d^2)}+o\left(\frac{x}{\log x}\right).$$

As in the proof of Lemma 2.3, one sees that

$$\sum_{\substack{y<d\leq Y\\ d|Y}} \frac{\rho_f(d^2)}{\phi(d^2)} = o(1)$$

and therefore

$$Q = \pi(x)\sum_{d|Y}\mu(d)\frac{\rho_f(d^2)}{\phi(d^2)} + o\left(\frac{x}{\log x}\right).$$

The function $\rho_f(d^2)/\phi(d^2)$ is multiplicative in d, hence

$$Q = \pi(x)\prod_{q\leq y}\left(1-\frac{\rho_f(q^2)}{\phi(q^2)}\right) + o\left(\frac{x}{\log x}\right)$$

and we conclude by Lemma 2.4. □

Lemma 2.6. *We have*

$$\#R = o\left(\frac{x}{\log x}\right).$$

Proof. First we observe that for any $\tau > 0$ we have

$$\#R \leq \sum_{p\leq x}\sum_{y<q\leq z}\delta(q^2|f(p)) = \sum_{y<q\leq x^{1/2-\tau}}\sum_{p\leq x}\delta(q^2|f(p)) + \sum_{x^{1/2-\tau}<q\leq z}\sum_{p\leq x}\delta(q^2|f(p)).$$

Let W and Z be the first and the second sum of the last expression, respectively. For W, Lemma 2.3 gives

$$W \leq \sum_{y<q\leq x^{1/2-\tau}}\left(1+\sum_{\substack{a\in(\mathbb{Z}/q^2\mathbb{Z})^\times\\ f(a)\equiv 0(q^2)}}\pi(x;q^2,a)\right) = O\left(\frac{x^{1/2-\tau}}{\log x}\right) + o\left(\frac{x}{\log x}\right) = o\left(\frac{x}{\log x}\right).$$

On Z we will use the trivial bound

$$\sum_{p\leq x}\delta(q^2|f(p)) \leq 1 + \sum_{\substack{n\leq x\\ (n,q^2)=1}}\delta(q^2|f(n)) \leq 1 + \frac{x}{q^2}\rho_f(q^2) + \rho_f(q^2)$$

which gives

$$\begin{aligned} Z &\leq \sum_{x^{1/2-\tau}<q\leq z}\left(1+\frac{x}{q^2}\rho_f(q^2)+\rho_f(q^2)\right)\\ &\leq z^{\varepsilon}\sum_{x^{1/2-\tau}<q\leq z}\left(\frac{x}{q^2}+1\right)\\ &\leq z^{\varepsilon}\pi(z)x^{2\tau} < z^{1+\varepsilon}x^{2\tau} \end{aligned}$$

for $z \gg_\varepsilon 1$. Recall $z = x^{1-\epsilon}$ where $\epsilon > 0$ is fixed. Taking $\varepsilon = \epsilon$ and $\tau = \epsilon^2/4$ gives $Z < x^{1-0.5\epsilon^2} = o(x/\log x)$, which concludes the proof. □

Finally, lemmas 2.5 and 2.6 together with equation (2) give

$$N_f(x) = c_f\frac{x}{\log x} + o\left(\frac{x}{\log x}\right) + O(\#S).$$

Since $S = \Sigma_x$ in the notation of Theorem 2.1, we see that in order to prove Theorem 1.1 it suffices to prove Theorem 2.1, as claimed.

As the reader already noticed, we have put no effort in obtaining a good error term. An explicit error term is possible at this point, but the bound that we will later give for $\#S$ is sufficiently rough to make such a labor unnecessary.

3. A reduction

We claim that in order to prove Theorem 2.1 (and hence, Theorem 1.1) it suffices to prove

Theorem 3.1. *Let f be an irreducible polynomial of degree $r \geq 2$ with integer coefficients, and fix $\epsilon > 0$ sufficiently small (any fixed $\epsilon \leq 1/(2(r+1))$ will work). Define*

$$S_x = \{p \leq x : \exists q > x^{1-\epsilon}, q^2 | f(p)\}.$$

Assume that the ABC conjecture for number fields holds for each number field $\mathbb{Q}(\alpha)$ where α varies over the roots of f. Then

$$\#S_x = o\left(\frac{x}{\log x}\right).$$

First we need

Lemma 3.2. *Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Let $1/2 > \epsilon > 0$. Then*

$$\#\{p < x : \exists q > x^{1-\epsilon}, q^2 | ap + b\} = o\left(\frac{x}{\log x}\right).$$

Proof. If p is large enough in terms of a, b (uniformly in x), then

$$|ap + b| \geq q^2 > x^{2-2\epsilon} > p^{2-2\epsilon} \gg |ap + b|^{2-2\epsilon},$$

a contradiction. Hence, the set in question actually has bounded cardinality. □

Lemma 3.3. *For $\epsilon > 0$ and $g \in \mathbb{Z}[t]$ define the set*

$$T_x^\epsilon(g) = \{p < x : \exists q > x^{1-\epsilon}, q^2 | g(p)\}.$$

Let $g, h \in \mathbb{Z}[t]$ be two coprime polynomials. There is a constant X depending only on g, h, ϵ such that for all $x > X$ we have

$$T_x^\epsilon(gh) \subseteq T_x^\epsilon(g) \cup T_x^\epsilon(h).$$

Proof. Let X be such that $X^{1-\epsilon}$ is larger than all the prime divisors of the resultant R of g and h (note that $R \neq 0$ because $(g, h) = 1$). Take any $x > X$ and let us check the inclusion. Consider a prime $p \in T_x^\epsilon(gh)$. Let $q > x^{1-\epsilon}$ be a prime such that $q^2 | g(p)h(p)$, which exists because $p \in T_x^\epsilon(gh)$. Without loss of generality, suppose that $q | g(p)$. We claim that $q \nmid h(p)$. On the contrary, if $q | h(p)$ then $q | R$ but $q > x^{1-\epsilon} > X^{1-\epsilon}$ which is larger than any prime divisor of R. Therefore $q \nmid h(p)$, thus $q^2 | g(p)$. This proves that $p \in T_x^\epsilon(g)$. □

The previous lemma shows that it suffices to prove Theorem 2.1 for irreducible polynomials (note that f from Theorem 2.1 has no repeated factor). On the other hand, Theorem 3.1 and Lemma 3.2 precisely cover the cases of irreducible polynomials. More precisely, in Theorem 2.1 one can take $\epsilon_0 = 1/(2(r+1))$ if the maximal degree among the irreducible factors of f is $r \geq 2$. Therefore, if we prove Theorem 3.1 we also obtain Theorem 2.1 and hence Theorem 1.1.

Theorem 3.1 will be proved in Section 6.

4. The ABC conjecture

Let K be a number field and write M_K for the set of all places of K. Let M_K^0 be the set of finite places, and M_K^∞ the set of infinite places. If $v \in M_K$ then we write $\| \cdot \|_v$ for the normalized norm at v, which for $\alpha \in K^*$ is defined by

$$\|\alpha\|_v = \begin{cases} [\mathcal{O}_K : \mathfrak{p}]^{-\mathrm{ord}_\mathfrak{p}(\alpha)} & \text{if } v \in M_K^0 \text{ corresponds to the prime ideal } \mathfrak{p} \subseteq \mathcal{O}_K \\ |\sigma(\alpha)| & \text{if } v \in M_K^\infty \text{ corresponds to the real embedding } \sigma : K \to \mathbb{R} \\ |\sigma(\alpha)|^2 & \text{if } v \in M_K^\infty \text{ corresponds to the non-real embedding } \sigma : K \to \mathbb{C} \end{cases}$$

and of course $\|0\|_v = 0$ in all cases. This is an absolute value except in the last case.

The *height (relative to K)* of $\alpha \in K$ is defined by

$$h_K(\alpha) = \sum_{v \in M_K} \log \max\{1, \|\alpha\|_v\}.$$

The *absolute height* is defined by

$$h(\alpha) = \frac{1}{[K:\mathbb{Q}]} h_K(\alpha)$$

and it only depends on α, not on the particular number field K (as long as it contains α). If S is a finite set of places, the *truncated counting function* for $\alpha \neq 0$ is defined by

$$N^{(1)}_{K,S}(\alpha) = \sum_{v \in M^0_K \setminus S} \min\{1, \max\{0, \mathrm{ord}_{\mathfrak{p}_v} \alpha\}\} \log[\mathcal{O}_K : \mathfrak{p}_v]$$

where $\mathfrak{p}_v$ is the prime corresponding to $v \in M^0_K$. The truncated counting function does depend on α, S and K even if we normalize by $1/[K:\mathbb{Q}]$ (which we do not) due to ramification.

With this notation, let us recall the ABC conjecture for number fields stated in the introduction.

Conjecture 4.1 (ABC for number fields)**.** *Let K be a number field. Let $\epsilon > 0$ and fix mutually distinct elements $b_1, \dots, b_M \in K$. Let S be a finite set of places of K. Then for all but finitely many $\alpha \in K$ one has*

$$(M - 2 - \epsilon) h_K(\alpha) < \sum_{i=1}^{M} N^{(1)}_{K,S}(\alpha - b_i).$$

For $x = a/b \in \mathbb{Q}^*$ with a and b coprime integers, we define the *radical of x* by $\mathrm{rad}(x) = \mathrm{rad}(a)$. Note that

$$\log \mathrm{rad}(x) = N^{(1)}_{\mathbb{Q},\emptyset}(x).$$

Given $F \in \mathbb{Q}[t]$ an irreducible monic polynomial of degree r, it will be convenient to define its height $H(F)$ as

$$H(F) = \exp(r h(\alpha))$$

where α is any root of F (the roots of F are Galois conjugate, hence, they have the same absolute height). This definition actually agrees with the (exponential of the) *Mahler measure* of aF where a is the least common denominator of the coefficients of F, and therefore our $H(F)$ is essentially the same as the naive (multiplicative projective) height of F, up to a bounded factor that only depends on the degree of F. See the discussion in Section 7.

Theorem 4.2. *Let $r \geq 2$ and let M be an integer. Fix $b_1, \dots, b_M \in \mathbb{Q}$ mutually distinct rational numbers and let $\epsilon > 0$. Let K be a number field of degree r over $\mathbb{Q}$. Assume that the ABC conjecture for number fields holds for K. For all monic irreducible polynomials $F \in \mathbb{Q}[t]$ of degree r with a root in K, the following holds:*

$$(M - 2r^2 + r - 2 - \epsilon) \log H(F) \leq \sum_{i=1}^{M} \log \mathrm{rad} F(b_i) + A$$

where A is a constant depending only on r, ϵ, K and the b_i, but it is independent of the particular F satisfying the previous requirements.

Before presenting the proof of this result, let us make a comment on how this application of the ABC conjecture compares to previous ones. Classically, the ABC conjecture is used to study the factorization of $F(b)$ when we fix a polynomial $F \in \mathbb{Z}[t]$ and we move the argument b (such results are due to Langevin [7]). An application of this type in the context of squarefree values of polynomials (not at prime arguments) was given in [2]. In [9] a refinement is necessary and F is also allowed to vary. The bound in [9] has the same quality as Langevin's bound when we vary b and F is fixed, and it has exponential dependence in the multiplicative height of F which is precisely what is needed for the purposes of [9], but too weak for our present goal. Here, instead, we *fix* arguments b_i and move the polynomial F to get a result with good dependence on F. Such an application of the ABC conjecture was already considered in [10] and Theorem 4.2 is an elementary instance for irreducible polynomials over $\mathbb{Q}$ instead of more general polynomials over a number field (nevertheless, the result becomes much cleaner in this case).

Proof. Let $F \in \mathbb{Q}[t]$ be a monic irreducible polynomial of degree r and let $\alpha \in K$ be a root of F. Note that α is not one of the b_i because F is irreducible and $b_i \in \mathbb{Q}$. Let P be the set of finite places of $\mathbb{Q}$ where some b_i has a pole or at least two b_i have the same reduction, and let S be the set of places of K lying above a place in P. Let P_α be the set of finite places in $\mathbb{Q}$ above which α has a pole, or at which the discriminant Δ_F of F vanishes.

If $v \in M_K^0$ then we write v for the corresponding normalized valuation on K, that is, $v(x) = \mathrm{ord}_{\mathfrak{p}}(x)$ where $\mathfrak{p}$ is the prime corresponding to v. If $p \in M_{\mathbb{Q}}^0$ (which we identify with a prime number) then we write v_p for the corresponding normalized (p-adic) valuation on $\mathbb{Q}$. We write $v^+(x) = \max\{0, v(x)\}$ and similarly for v_p. For notational convenience, for $v \in M_K^0$ let us write $\deg(v)$ instead of $\log[\mathcal{O}_K : \mathfrak{p}]$, where $\mathfrak{p}$ is the prime corresponding to v (this notation is standard in Arakelov theory).

We have (the second-last equation will be explained below)

$$\begin{aligned} N_{K,S}^{(1)}(\alpha - b_i) &= \sum_{v \in M_K^0 \setminus S} \min\{1, v^+(\alpha - b_i)\} \deg(v) \\ &= \sum_{p \in M_{\mathbb{Q}}^0 \setminus P} \sum_{v|p} \min\{1, v^+(\alpha - b_i)\} \deg(v) \\ &= \sum_{p \in M_{\mathbb{Q}}^0 \setminus (P \cup P_\alpha)} \sum_{v|p} \min\{1, v^+(\alpha - b_i)\} \deg(v) + \sum_{p \in P_\alpha \setminus P} \sum_{v|p} \min\{1, v^+(\alpha - b_i)\} \deg(v) \\ &= \sum_{p \in M_{\mathbb{Q}}^0 \setminus (P \cup P_\alpha)} \min\{1, v_p^+(F(b_i))\} \log(p) + \sum_{p \in P_\alpha \setminus P} \sum_{v|p} \min\{1, v^+(\alpha - b_i)\} \deg(v) \\ &\leq \log \mathrm{rad} F(b_i) + \sum_{p \in P_\alpha \setminus P} \sum_{v|p} \min\{1, v^+(\alpha - b_i)\} \deg(v). \end{aligned}$$

Let us explain the step from the third to the fourth line. In Lemma 4.5 [10] it is shown that if $x \in K$ generates $K/\mathbb{Q}$, is regular above a prime p and the discriminant of the minimal polynomial H of x does not vanish at p, then one of the following holds:

- $v_p(H(0)) = 0$ and for each $v|p$ in K one has $v(x) = 0$, or
- there is exactly one $v_*|p$ in K such $v_*(x) > 0$ and $v(x) = 0$ for all other $v|p$. Moreover, $v_*(x) = v_p(H(0))$ and $\deg(v) = \log p$.

To get the fourth line from the third, one uses this result with $x = \alpha - b_i$ for each $p \notin P \cup P_\alpha$; such choice is allowed by definition of P and P_α. Note that indeed $K = \mathbb{Q}(x)$ since F is irreducible of degree $r = [K : \mathbb{Q}]$, that $H(t) = F(t + b_i)$ is the minimal polynomial of $\alpha - b_i$ and that the discriminant of H is Δ_F.

The ABC conjecture for K gives that for all but finitely many such F the following holds

$$\begin{aligned} (M - 2 - \epsilon) h_K(\alpha) &\leq \sum_{i=1}^{M} N_{K,S}^{(1)}(\alpha - b_i) \\ &\leq \sum_{i=1}^{M} \log \mathrm{rad} F(b_i) + \sum_{i=1}^{M} \sum_{p \in P_\alpha \setminus P} \sum_{v|p} \min\{1, v^+(\alpha - b_i)\} \deg(v). \end{aligned}$$

For $p \in M_{\mathbb{Q}}^0 \setminus P$ fixed, we know that at most one $v^+(\alpha - b_i)$ is non-zero because the b_i do not agree at p. Hence

$$\sum_{i=1}^{M} \sum_{p \in P_\alpha \setminus P} \sum_{v|p} \min\{1, v^+(\alpha - b_i)\} \deg(v) \leq \sum_{p \in P_\alpha \setminus P} \sum_{v|p} \deg(v) \leq r \sum_{p \in P_\alpha} \log p.$$

Counting the zeros of Δ_F and poles of α we get

$$\sum_{p \in P_\alpha} \log p \leq h(\Delta_F) + h_K(\alpha) \leq 2(r-1) r h(\alpha) + O_r(1) + h_K(\alpha) = (2r - 1) h_K(\alpha) + O_r(1)$$

where we used the bound $h(\Delta_F) \leq 2(r-1)rh(\alpha) + O_r(1)$ which can be proved by expressing Δ_F in terms of the roots of F. Hence

$$(M - 2 - \epsilon)h_K(\alpha) < \sum_{i=1}^{M} \log \mathrm{rad} F(b_i) + (2r-1)rh_K(\alpha) + O_r(1)$$

that is

$$(M - 2r^2 + r - 2 - \epsilon)h_K(\alpha) < \sum_{i=1}^{M} \log \mathrm{rad} F(b_i) + O_r(1).$$

We can increase the implicit constant in the error term $O_r(1)$ to a new constant A such that the inequality holds for all F that satisfy our requirements (that is, to include the finitely many exceptions). This A will depend on r, K, ϵ and the b_i (hence M), but it will be uniform for F. Recalling that $h_K(\alpha) = rh(\alpha) = \log H(F)$, we conclude the proof. □

5. Arithmetic progressions of primes

The celebrated Green-Tao theorem [4] asserts that every set of primes with positive upper density (among primes) has arithmetic progressions of any length. This result was later refined in a number of directions. Here we need the following improvement due to Tao and Ziegler (see Theorem 1.3 and Remark 1.4 in [11], see also [12]).

Theorem 5.1. *Let P be a set of primes with positive upper density in the primes, that is*

$$\limsup_{x\to\infty} \frac{\#\{p \in P : p \leq x\}}{\pi(x)} > 0.$$

Let $\epsilon > 0$ and k a positive integer as large as we want. There are infinitely many k-terms arithmetic progressions of the form

$$p, p+d, p+2d, \ldots, p+(k-1)d$$

where all the terms belong to P, and $0 < d < p^{\epsilon}$.

Such a result without the restriction $d < p^{\epsilon}$ was proved by Green and Tao [4], but for our application the parameter ϵ is crucial. Note that the Tao-Ziegler theorem is more general and holds for polynomial progressions, but here we just need the case of arithmetic (linear) progressions. Indeed, Tao and Ziegler remark (see Remark 2.4 [11]) that the argument of Green and Tao [4] can be modified to get such a result in the linear case, which is all we need.

6. Proof of Theorem 1.1

Recall that for proving Theorem 1.1 it suffices to prove Theorem 3.1. That is, on the ABC conjecture for number fields, we want to give an upper bound for $\#S_x$ of the form $o(x/\log x)$, where

$$S_x = \{p \leq x : \exists q > x^{1-\epsilon}, q^2 | f(p)\}.$$

Here, $f \in \mathbb{Z}[t]$ satisfies the hypotheses from Theorem 3.1 (namely, it is irreducible of degree $r \geq 2$). Define

$$P = \{p : \exists q > p^{1-\epsilon}, q^2 | f(p)\},$$

then $S_x \subseteq \{p \in P : p \leq x\}$. Thus, in order to prove Theorem 1.1 it suffices to show (on the ABC conjecture) that for suitable $\epsilon > 0$ the set P satisfies

$$\#P \cap [0, x] = o\left(\frac{x}{\log x}\right),$$

or in other words, that P has density 0 in the primes. We will do this by using the results of Green, Tao and Ziegler from the previous section.

Let a be the leading coefficient of f. For n, d positive integers, define $f_{n,d}$ as the polynomial

$$f_{n,d}(t) = \frac{1}{d^r a} f(n + td).$$

For the next claim, recall our convention on the height of a monic irreducible polynomial in $\mathbb{Q}[t]$ (see Section 4).

Claim 6.1. *The polynomial $f_{n,d} \in \mathbb{Q}[t]$ is monic irreducible of degree r. If α is a root of f then $(\alpha - n)/d$ is a root of $f_{n,d}$, it generates $K = \mathbb{Q}(\alpha)$ over $\mathbb{Q}$, and one has*

$$H(f_{n,d}) \geq \frac{n^r}{4^r d^r H(f/a)}.$$

Proof. That $f_{n,d}$ is monic of degree r is clear. A direct computation shows the statement about the root, and now Galois theory implies irreducibility. The height bound also follows from the relation on the roots:

$$\log H(f_{n,d}) = rh\left(\frac{\alpha - n}{d}\right) \geq r(h(n) - h(\alpha) - h(d) - \log 4) = \log n^r - \log H(f/a) - \log d^r - \log 4^r.$$

□

Let $M = 6r^3 + 1$ and fix any $\epsilon \leq 1/(2(r+1))$ in the definition of P.

Claim 6.2. *Assume that the ABC conjecture for number fields holds for $\mathbb{Q}(\alpha)$, where α is a root of f. For all sufficiently large primes $p \in P$, and for all integers $0 < d < p^\epsilon$, we have that some of the numbers*

$$p, p + d, \ldots, p + (M-1)d$$

is not in P.

Proof. Suppose that there are arbitrarily large $p \in P$ such that for each such p there is d_p with $0 < d_p < p^\epsilon$ satisfying that

$$p, p + d_p, \ldots, p + (M-1)d_p \in P.$$

We will obtain a contradiction from this assumption, thus proving the claim. Take any such an element $p \in P$, then the ABC conjecture and Theorem 4.2 applied to $K = \mathbb{Q}(\alpha)$ and $F = f_{p,d_p}$ give (choose $b_j = j - 1$ and $\epsilon = 1$ in Theorem 4.2; not to be confused with the ϵ in the present claim)

$$(M - 3r^2) \log H(f_{p,d_p}) \leq \sum_{j=1}^{M} \log \mathrm{rad} f_{p,d_p}(j-1) + A$$

for some constant A independent of p and d_p. Indeed, the constant A only depends on f because both M and the number field K are determined by f.

Claim 6.1 and the assumption that $p + (j-1)d_p \in P$ for each $1 \leq j \leq M$ give

$$\begin{aligned}
(M - 3r^2) \log \frac{p^r}{4^r d_p^r H(f/a)} &\leq \sum_{j=1}^{M} \log \mathrm{rad} f_{p,d_p}(j-1) + A \\
&= \sum_{j=1}^{M} \log \mathrm{rad} \frac{1}{d_p^r a} f(p + (j-1)d_p) + A \\
&\leq \sum_{j=1}^{M} \log \mathrm{rad} f(p + (j-1)d_p) + A \\
&\leq \sum_{j=1}^{M} \log \left| \frac{f(p + (j-1)d_p)}{(p + (j-1)d_p)^{1-\epsilon}} \right| + A.
\end{aligned}$$

Observe that

$$\log \frac{p^r}{4^r d_p^r H(f/a)} = r \log \frac{p}{d_p} + O_f(1)$$

where the implicit constant only depends on (the degree and coefficients of) f, and moreover the triangle inequality gives

$$\log \left| \frac{f(p + (j-1)d_p)}{(p + (j-1)d_p)^{1-\epsilon}} \right| \leq \log \left| (p + (j-1)d_p)^{r-1+\epsilon} \right| + O_f(1).$$

These estimates together with the fact that M only depends on $r = \deg f$, give

$$(M - 3r^2)r \log \frac{p}{d_p} \leq \sum_{j=1}^{M} \log \left|(p + (j-1)d_p)^{r-1+\epsilon}\right| + O_f(1)$$

as p grows to infinity, where the implicit constant is independent of p and d_p. Since $0 < d_p < p^\epsilon$, we deduce

$$(1-\epsilon)(M - 3r^2)r \log p < (r - 1 + \epsilon)M \log p + O_f(1)$$

hence

$$\left(M - 3r^3 - \epsilon M(r+1) + 3\epsilon r^2\right) \log p < O_f(1).$$

Recalling that $\epsilon \leq 1/(2(r+1))$ we see that

$$\left(M/2 - 3r^3\right) \log p < O_f(1).$$

Since $M = 6r^3 + 1$, we get a contradiction for large p. □

By Theorem 5.1, we see that Claim 6.2 proves (on the ABC conjecture) that P cannot have positive upper density in the primes. Hence P has density zero in the primes, which concludes the proof of Theorem 1.1 as explained in the beginning of this section.

7. Further applications of ABC

In this section we briefly present a variation of Theorem 4.2. This result is not needed for the proof of Theorem 1.1, however, it is of independent interest and can be useful in other applications. The theorem that we discuss below is a particular instance of the results in [10], but when it is formulated for polynomials over $\mathbb{Q}$ the statement becomes much simpler and it oughts to be stated explicitly.

Theorem 7.1. *Assume Vojta's ABC conjecture for algebraic numbers of bounded degree (see Conjecture 2.3 in* [13] *and Conjecture 25.3.b in* [14] *in the case of the projective line). Let $r \geq 2$ and let M be an integer. Fix $b_1, \ldots, b_M \in \mathbb{Q}$ mutually distinct rational numbers and let $\epsilon > 0$. For all monic irreducible polynomials $F \in \mathbb{Q}[t]$ of degree r, the following holds:*

$$(M - 2r^2 - r - \epsilon) \log H(F) \leq \sum_{i=1}^{M} \log \mathrm{rad} F(b_i) + A$$

where A is a constant depending only on r, ϵ and the b_i, but it is independent of the particular F satisfying the previous requirements.

The term $-2r^2 - r$ comes from estimating the logarithmic discriminant of a root of F in terms of heights, as in [10]. Details of the proof are similar to the computations in the previous section, and we leave them to the reader (alternatively, see [10]).

Remarks.

- Note that we get a stronger conclusion (a height inequality without fixing the field generated by a root of F) at the cost of assuming Vojta's ABC conjecture for bounded degree, which is stronger than the number field ABC conjecture required for Theorem 4.2.
- Of course, in applications one can always factor the relevant polynomials into irreducible factors and apply the result to each one.
- It can be useful to replace $H(F)$ by a slightly different height which is simpler to compute, let us indicate how. Given $F = a_n t^n + \ldots + a_1 t + a_0 \in \mathbb{Q}[t]$, define its *naive (multiplicative, projective) height* by

  $$H_m(F) = \prod_{v \in M_\mathbb{Q}} \max_{0 \leq i \leq n} \{\|a_i\|_v\}.$$

  Note that $H_m(xF) = H_m(F)$ for any $x \in \mathbb{Q}^*$, and if F has coprime integer coefficients a_i then $H_m(F) = \max_i |a_i|$. If F is monic and irreducible then

  $$c_1 H_m(F) \leq H(F) \leq c_2 H_m(F)$$

  for certain constants c_1, c_2 that depend only on $\deg F$, see Proposition 4 in p.49 [6].

8. Acknowledgments

This work is part of my PhD Thesis at Queen's University. I would like to thank my supervisor Ram Murty for suggesting to look at the problem of counting squarefree values of polynomials at primes.

Most of this research was partially supported by an Ontario Graduate Scholarship at Queen's University. The final revisions were made with the support of a Benjamin Peirce Fellowship at Harvard University.

References

[1] E. Bombieri, W. Gubler, *Heights in Diophantine geometry*. New Mathematical Monographs, 4. Cambridge University Press, Cambridge, 2006. xvi+652 pp. ISBN: 978-0-521-84615-8; 0-521-84615-3.

[2] A. Granville, *ABC allows us to count squarefrees*. Internat. Math. Res. Notices 1998, no. 19, 991-1009.

[3] A. Granville, H. Stark, *abc implies no "Siegel zeros" for L-functions of characters with negative discriminant*. Invent. Math. 139 (2000), no. 3, 509-523.

[4] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*. Ann. of Math. (2) 167 (2008), no. 2, 481-547.

[5] H. Helfgott, *Square-free values of $f(p)$, f cubic*. Preprint.

[6] S. Lang, *Diophantine geometry*. Interscience Tracts in Pure and Applied Mathematics, No. 11 Interscience Publishers, New York-London 1962 x+ 170 pp.

[7] M. Langevin, *Cas d'égalité pour le théorème de Mason et applications de la conjecture (abc)*. C. R. Acad. Sci. Paris Sér. I Math. 317 (1993), no. 5, 441-444.

[8] J. Lee, M. R. Murty, *Dirichlet series and hyperelliptic curves*. Forum Math. 19 (2007), no. 4, 677-705.

[9] M. R. Murty, H. Pasten, *Counting squarefree values of polynomials with error term*, IJNT (2014), DOI: 10.1142/S1793042114500535.

[10] H. Pasten, *Powerful values of polynomials and a conjecture of Vojta*. J. Number Theory 133 (2013), no. 9, 2964-2998.

[11] T. Tao, T. Ziegler, *The primes contain arbitrarily long polynomial progressions*. Acta Math., 201 (2008), 213-305.

[12] T. Tao, T. Ziegler, *Erratum to "The primes contain arbitrarily long polynomial progressions"*. Acta Math., 210 (2013), 403-404.

[13] P. Vojta *A more general abc conjecture*, Internat. Math. Res. Notices, 1998 (1998), 1103-1116.

[14] P. Vojta *Diophantine approximation and Nevanlinna theory*, Arithmetic geometry, 111-224, Lecture Notes in Math., 2009, Springer, Berlin (2011).

Department of Mathematics, Harvard University
1 Oxford Street
Cambridge, MA 02138 USA
E-mail address: hpasten@gmail.com