ABC ALLOWS US TO COUNT SQUAREFREES

ANDREW GRANVILLE

Dedicated to the memory of Paul Erdős

ABSTRACT. We show several consequences of the *abc*-conjecture for questions in analytic number theory which were of interest to Paul Erdős: For any given polynomial $f(x) \in \mathbb{Z}[x]$, we deduce, from the *abc*-conjecture, an asymptotic estimate for the frequency with which $f(n)$ is squarefree, when n is an integer (and also deduce such estimates for binary homogenous forms). Amongst several applications of this result, we deduce that there is a squarefree number in every interval of length $O(x^\varepsilon)$ around x, and give the asymptotic formula, predicted by Erdős, for the average moments for the gaps between squarefree numbers.

1. INTRODUCTION.

For any given polynomial $f(x) \in \mathbb{Z}[x]$, we investigate what proportion of the integers $f(1), f(2), f(3), \dots$ are squarefree[1]?

The values, at integers, taken by certain polynomials, are always divisible by a square for not entirely obvious reasons (for example $n(n-1)(n-2)(n-3)$ is always divisible by 8). We take care of this as follows: Let B be the greatest common divisor of $f(n)$, $n \in \mathbb{Z}$; and let B' be the smallest divisor of B such that B/B' is squarefree. Then $f(n)/B'$ can feasibly be squarefree for various integers n.

The study of this question has a rich history. It was Erdős [5] who established that if $f(x)$ has degree ≤ 3, and $B = 1$, then there are infinitely many integers n for which $f(n)$ is squarefree. There are no such results proven unconditionally for any irreducible polynomials of degree > 3, though Browkin, Filaseta, Greaves and Schinzel [2] did prove such a result for all cyclotomic polynomials under the assumption of the *abc*-conjecture.

Similar results for binary homogenous forms, whose irreducible factors have low degree, were established by Hooley [14], by Greaves [13], and by Browkin, Filaseta, Greaves and Schinzel [2]. Here we show that these questions can be completely answered, as a consequence of the *abc*-conjecture, which we now describe:

The *abc*-conjecture. *(Oesterlé, Masser, Szpiro): Fix $\varepsilon > 0$. If a, b, c are coprime positive integers satisfying $a + b = c$ then*

$$c \ll_\varepsilon N(a,b,c)^{1+\varepsilon}, \tag{1}$$

A Presidential Faculty Fellow. Also supported, in part, by the National Science Foundation.

[1] That is, not divisible by the square of a prime

where $N(a,b,c)$ is the product of the distinct primes dividing abc.

This conjecture has many extraordinary consequences (such as Fermat's Last Theorem, other than perhaps finitely many examples). Following constructions of Belyi [1] and Elkies [3], and a little bit of elementary sieving, we shall prove several results about the distribution of squarefree integers, as a consequence of the abc–conjecture.

Theorem 1. *Suppose that $f(x) \in \mathbb{Z}[x]$, without any repeated roots. Let B be the largest integer which divides $f(n)$ for all integers n; and select B' to be the smallest divisor of B for which B/B' is squarefree. If the abc-conjecture is true then there are $\sim c_f N$ positive integers $n \le N$ for which $f(n)/B'$ is squarefree, where $c_f > 0$ is a positive constant, which we determine as follows:*

$$c_f \ = \ \prod_{p \text{ prime}} \left(1 - \frac{\omega_f(p)}{p^{2+q_p}}\right)$$

where, for each prime p, we let q_p be the largest power of p which divides B', and let $\omega_f(p)$ denote the number of integers a in the range $1 \le a \le p^{2+q_p}$ for which $f(a)/B' \equiv 0 \pmod{p^2}$.

This result can be proved unconditionally if f has degree ≤ 2 using the sieve of Eratosthenes. It was proved unconditionally by Hooley [14] for f of degree 3.

Theorem 1 can be viewed as verifying the appropriate "local-global" principle: The factors $\left(1 - \frac{\omega_f(p)}{p^{2+q_p}}\right)$ represent the proportion of integers n for which $f(n)/B'$ is not divisible by p^2. We have thus shown that the proportion of positive integers n for which $f(n)/B'$ is squarefree is exactly the product, over all primes p, of these local densities.

As we noted above, there has also been considerable interest in squarefree values of binary forms. The proof of the following result is a modification of that of Theorem 1, though strangely involves the classification of the finite subgroups of $\mathrm{PGL}(2,\mathbb{Q})$ (see the Appendix):

Theorem 2. *Suppose that $f(x,y) \in \mathbb{Z}[x,y]$ is homogenous, without any repeated linear factors. Let B be the largest integer which divides $f(m,n)$ for all pairs of integers m,n; and select B' to be the smallest divisor of B for which B/B' is squarefree. We will assume that $M,N \to \infty$ in the following[2]. If the abc-conjecture is true then there are $\sim c'_f MN$ pairs of positive integers $m \le M$, $n \le N$ for which $f(m,n)/B'$ is squarefree, where $c'_f > 0$ is a positive constant, which we determine as follows:*

$$c'_f \ = \ \prod_{p \text{ prime}} \left(1 - \frac{\omega'_f(p)}{p^{4+2q_p}}\right)$$

where, for each prime p, we let q_p be the largest power of p which divides B', and let $\omega_f(p)$ denote the number of pairs of integers a,b in the range $1 \le a,b \le p^{2+q_p}$ for which $f(a,b)/B' \equiv 0 \pmod{p^2}$.

[2] If one of these variables does not go to infinity then the desired result may be obtained by summing over applications of Theorem 1

We again note the "local-global" principle in action here. Theorems 1 and 2 above carry over, with no significant changes, to arbitrary number fields K; that is, one can state analogous results for $f(x) \in K[x]$ and $f(x,y) \in K[x,y]$, though one needs to give an appropriate formulation of the *abc*-conjecture in number fields[3].

A similar proof allows us to solve various questions about the distribution of squarefree numbers: Let $s_1 = 1 < s_2 = 2 < s_3 = 3 < s_4 = 5 < \dots$ be the sequence of squarefree numbers. Filaseta and Trifonov [9] have shown that consecutive squarefree numbers cannot get too far apart: that is, $s_{n+1} - s_n \ll s_n^{1/5} \log(s_n)$. Assuming the *abc*-conjecture we can get a sharper result:

Theorem 3. *Suppose that the abc-conjecture is true and fix $\varepsilon > 0$. Then, once x is sufficiently large, there must be a squarefree integer in the interval $(x, x + x^{\varepsilon})$. In other words, $s_{n+1} - s_n \ll_{\varepsilon} s_n^{\varepsilon}$.*

Let $a_1 < a_2 < \cdots < a_k$ be a fixed set of positive integers. From the sieve of Eratosthenes one can show that there are $\sim \gamma_{\underline{a}} x$ integers $m \le x$ for which $m, m + a_1, m + a_2, \dots, m + a_k$ are all squarefree, where the constant

$$\gamma_{\underline{a}} = \gamma_{\{a_1,a_2,\dots,a_k\}} = \prod_p \left(1 - \frac{\omega_{\underline{a}}(p)}{p^2}\right),$$

and $\omega_{\underline{a}}(p)$ is the number of distinct residue classes in the set $0, a_1, \dots, a_k \pmod{p^2}$. Thus there are $\sim \delta_t x$ squarefree integers $n \le x$ for which the next largest squarefree integer is $n + t$, where

$$\delta_t := \sum_{I \subset \{1,2,\dots,t-1\}} (-1)^{|I|} \gamma_{I \cup \{0,t\}},$$

which is easily proved using the inclusion-exclusion formula.

It was Erdős [4] who began the study of the average moments of $s_{n+1} - s_n$; that is, $\frac{1}{x}\sum_{s_n \le x} (s_{n+1} - s_n)^A$, showing that this tends to a limit as $x \to \infty$ for $0 \le A \le 2$; this was extended to $A \le 3$ by Hooley [15], to $A \le 29/9$ by Filaseta [8], and to $A \le 43/13$ by Filaseta and Trifonov [10]. If we define $S(x;t)$ to be the number of $s_n \le x$ for which $s_{n+1} - s_n = t$ then the above sum equals $\frac{1}{x}\sum_{t \ge 1} S(x;t) t^A$. In section 6, we will deduce that

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

from the *abc*-conjecture. Therefore

$$\frac{1}{x}\sum_{s_n \le x} (s_{n+1} - s_n)^A = \frac{1}{x}\sum_{1 \le t \le T} S(x;t) t^A + O\left(\frac{1}{T}\right) \to \sum_{1 \le t \le T} \delta_t t^A + O\left(\frac{1}{T}\right),$$

as $x \to \infty$. Now letting $T \to \infty$, and defining $\beta_A := \sum_{t \ge 1} \delta_t t^A$, we deduce the following theorem:

[3] Vojta [22, page 84] showed how to formulate the *abc*-conjecture in arbitrary number fields; from which Elkies [3] elegantly deduced Faltings' Theorem.

Theorem 4. *Suppose that the abc-conjecture is true. For any fixed $A > 0$ there exists a constant $\beta_A > 0$ such that*

$$\sum_{s_n \le x} (s_{n+1} - s_n)^A \sim \beta_A x.$$

Remark. In fact Theorem 4 follows from Theorem 3 as was shown in [8]. We give a simplified version of that deduction here.

All of these results rely on the following consequence of Belyi's Theorem, first noted by Elkies [3,(26)] and Langevin [17] (a proof is also sketched in section 3):

Theorem 5. *Assume that the abc-conjecture is true. Suppose that $f(x,y) \in \mathbb{Z}[x,y]$ is homogenous, without any repeated linear factors. Fix $\varepsilon > 0$. Then, for any coprime integers m and n,*

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

Note that the constant implicit in "$\gg$" depends on both ε and f.

Remark. The *abc*-conjecture is the case $f(x,y) = xy(x+y)$ of the estimate in Theorem 5. Roth's Theorem also follows easily from this estimate, since $|f(m,n)|$ is at least as large as the product of the primes dividing it.

Theorem 5 is "best possible" for any such $f(x,y) \in \mathbb{Z}[x,y]$ of degree > 2; that is, one can always find coprime integers m, n with $\prod_{p|f(m,n)} p \ll \max\{|m|, |n|\}^{\deg(f)-2}$. One can prove this via a standard "pigeonhole principle" argument: let ℓ be the smallest prime which does not divide the discriminant of $f(x,1)$, and such that there exists an integer $t \not\equiv 0 \pmod{\ell}$ with $f(t,1) \equiv 0 \pmod{\ell}$. We can use the Hensel lifting lemma to determine t_k such that $f(t_k, 1) \equiv 0 \pmod{\ell^k}$ for any given positive integer k. There are more than ℓ^{2k} integers $a - bt_{2k}$ with $0 \le a, b \le \ell^k$ so two of them are congruent $\pmod{\ell^{2k}}$, and we let $m - nt_{2k}$ be their difference. If ℓ^r is the highest power of ℓ dividing both m and n and $M = m/(m,n)$, $N = n/(m,n)$ then we find that $f(M,N) \equiv 0 \pmod{\ell^{2k-r}}$ whereas $\max\{|M|, |N|\}^2 \le (\ell^{k-r})^2 \le \ell^{2k-r}$, establishing the result.

If we wish to consider $g(x) \in \mathbb{Z}[x]$, then we can obtain a stronger consequence of Theorem 5 than comes from simply setting $n = 1$. If $g(x)$ has degree d then we let $f(x,y) = y^{d+1} g(x/y)$; thus $g(x) = f(x,1)$, but f has one higher degree than before. So now, applying Theorem 5, we obtain:

Corollary 1. *Assume that the abc-conjecture is true. Suppose that $g(x) \in \mathbb{Z}[x]$ has no repeated roots. Fix $\varepsilon > 0$. Then*

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

(This result was also noted by Langevin [17].) By a similar counting argument to the one following Theorem 5, one can show that this result is "best possible"; that is, one can always find arbitrarily large integers m with $\prod_{p|g(m)} p \ll |m|^{\deg(g)-1}$.

The next result, although an immediate corollary to Theorem 5 and Corollary 1, seems to be of independent interest.

Theorem 6. *Assume that the abc-conjecture is true. Suppose that $f(x,y) \in \mathbb{Z}[x,y]$ is homogenous, without any repeated linear factors. Fix $\varepsilon > 0$. If q^2 divides $f(m,n)$, for any coprime integers m and n then $q \ll \max\{|m|,|n|\}^{2+\varepsilon}$. Also, if $g(x) \in \mathbb{Z}[x]$ has no repeated roots and q^2 divides $g(m)$, then $q \ll |m|^{1+\varepsilon}$.*

We do not yet know, in general, whether this result is best possible, though we expect so:

Conjecture. *Suppose that $f(x,y) \in \mathbb{Z}[x,y]$ is homogenous, without any repeated linear factors, of degree ≥ 4. There exist infinitely many pairs of coprime integers m and n, for which there is an integer $q \gg \max\{|m|,|n|\}^2$ with q^2 dividing $f(m,n)$. Similarly, for any $g(x) \in \mathbb{Z}[x]$ without repeated roots of degree ≥ 2 there are arbitrarily large integers m for which there is an integer $q \gg m$ with q^2 dividing $g(m)$.*

Using a "pigeonhole principle" argument as above, one only gets $q \gg \max\{|m|,|n|\}$ with q^2 dividing $f(m,n)$, and $q \gg \sqrt{m}$ with q^2 dividing $g(m)$, respectively.

We can, however, prove our Conjecture when f has degree 4 (and when g has degree 2): Any equation $cv^2 = f(u,1)$ describes a curve of genus 1. If this has infinitely many rational points (as must happen for well chosen values of integer c), we can write them each in the form $(m/n, r/n^2)$ and then get the desired examples since $f(m,n) = cr^2$.

The first result in Theorem 6 implies that if $f(x)$ has degree > 4 then there are only finitely many rational solutions to $y^k = f(x)$ for any fixed $k \geq 2$; a result which follows from Faltings' Theorem. The second result in Theorem 6 implies that if $f(x)$ has degree > 2 then there are only finitely many integer solutions to $y^k = f(x)$ for any fixed $k \geq 2$; a result which follows from the Thue-Siegel Theorem. However we can conclude somewhat more:

An integer n is called *powerful* if p^2 divides n for every prime p dividing n. The first result in Theorem 6 implies that if $f(x,y) \in \mathbb{Z}[x,y]$ has degree > 4 then $f(m,n)$, with $(m,n) = 1$, is powerful only finitely often. Similarly, the second result in Theorem 6 implies that if $g(x) \in \mathbb{Z}[x]$ has degree > 2 then $g(m)$ is powerful only finitely often.

Let $r_1 = 1 < r_2 = 4 < \ldots$ be the sequence of powerful numbers. If we let $x + y\sqrt{8} = (3+\sqrt{8})^k$, for any integer k, then both $8y^2$ and $x^2 = 8y^2 + 1$ are powerful. Thus there are infinitely many integers n for which $r_{n+1} - r_n = 1$. Erdős [6] conjectured that there are never three consecutive powerful numbers; that is $r_{n+2} - r_n > 2$. It follows easily from the *abc*-conjecture that there are only finitely many such triples, for if $t-1, t, t+1$ are all powerful, then apply the *abc*-conjecture to the equation $1 + (t^2 - 1) = t^2$ to get a contradiction. In fact the *abc*-conjecture implies rather more:

Theorem 7. *Assume that the abc-conjecture is true. If $r_1 = 1 < r_2 = 4 < \ldots$ is the sequence of powerful numbers then $r_{n+2} - r_n \to \infty$ as $n \to \infty$.*

To prove this, suppose it were false, so that there exist integers $0 < a < b$ for which there are infinitely many integers m with $m, m+a$ and $m+b$ all powerful. But then for $g(x) = x(x+a)(x+b)$, we have $\prod_{p|g(m)} p \ll m^{3/2}$, contradicting Corollary 1.

It is an open question to try to estimate the number of $r_n \le x$ for which $r_{n+1} - r_n = 1$; in other words, to estimate the number of pairs of consecutive powerful numbers up to x. The above construction gives $\gg \log x$ such pairs, and one might guess that there are $\sim c \log x$ for some constant $c > 0$.

We can also apply Corollary 1 to binomial coefficients, to get: For any fixed integer $k \ge 3$, there are only finitely many integers n for which $\binom{n}{k}$ is powerful. In fact, Erdős and Selfridge conjectured that the only example with $3 \le k \le n/2$ is $\binom{50}{3}$; which we verified in [11] for $n < 10^6$. We also showed there, assuming the abc-conjecture, that there are, in all, only finitely many pairs of integers k, n satisfying $3 \le k \le n/2$, for which $\binom{n}{k}$ is powerful.

It has long been known that if $d := (2n+1)^r - 1$ is squarefree, with $n > 1$ then the class group of $\mathbb{Q}(\sqrt{-d})$ contains an element of order r; and, similarly, if $D := (2N+1)^{2R} + 1$ is squarefree, with $N > 1$ then the class group of $\mathbb{Q}(\sqrt{D})$ contains an element of order R. As noted by Ram Murty in [18], we can thus deduce from the abc-conjecture, via Theorem 1, quantitative lower bounds for the number of such quadratic fields. Subsequently Murty [19] cleverly dispensed with the assumption of the abc-conjecture, and even got sharper lower bounds, by finding a more elaborate class of such fields, allowing him to directly apply the tools of sieve theory.

Murty's approach to lower bounds for the number of such real quadratic fields amounts to giving a lower bound for the number of distinct values of $f(n)$ in $\mathbb{Q}/\mathbb{Q}^2$, with $1 \le n \le N$, for certain polynomials f. From Theorem 1 we immediately deduce

Corollary 2. *Assume that the abc-conjecture is true, and that $f(x) \in \mathbb{Z}[x]$ has no repeated roots. Then there are $\gg_f N$ distinct values of $f(n)$ in $\mathbb{Q}/\mathbb{Q}^2$, with $1 \le n \le N$.*

We guess that the number of such distinct values is $\sim c'_f N$ for some constant $c'_f \ge c_f > 0$, though we are not sure what c'_f should equal.

The result in Corollary 2 follows unconditionally when f has degree ≤ 3, from the remarks immediately following the statement of Theorem 1. By modifying Murty's argument in [18], one has, in general, the unconditional lower bound $\gg_f N/\log^{\gamma_f} N$ distinct values of $f(n)$ in $\mathbb{Q}/\mathbb{Q}^2$, with $1 \le n \le N$, where $\gamma_f \ge 1$ is the number of distinct irreducible factors of f: The fundamental lemma of the sieve, together with the Cebotarev density theorem[4] gives that if u is a sufficiently large, fixed, real number (depending on f) then there are $\asymp_{u,f} N/\log^{\gamma_f} N$ integers n, with $N/2 \le n \le N$, for which $f(n)/B$ is free of prime factors $< N^{1/u}$. Thus if $f(n) \in a\mathbb{Q}^2$, for such an integer n, where a is squarefree then a has $\ll u \deg f + \log B \ll_f 1$ prime factors. Now, Theorem 1b of Evertse and Silverman [7], implies that the number of integer solutions to $Ay^2 = f(x)$ is bounded as a function of the number of distinct prime factors of A. Therefore no more than an absolutely bounded number of such n give rise to the same value of $f(n)/B$ in $\mathbb{Q}/\mathbb{Q}^2$, and our result follows.

The proof of the key result, Theorem 5, follows easily from the following:

[4] Used to estimate the Euler product that arises

Lemma 1. *Given any homogenous $f(x,y) \in \overline{\mathbb{Q}}[x,y]$ we can determine homogenous polynomials $a(x,y), b(x,y), c(x,y) \in \mathbb{Z}[x,y]$ all of degree $D \geq 1$, without common factors, where $a(x,y)b(x,y)c(x,y)$ has exactly $D+2$ non–proportional linear factors, including the factors of $f(x,y)$, and $a(x,y)+b(x,y)=c(x,y)$.*

2. Sketch of the Proof of Lemma 1.

Belyi's theorem [1, 21 pg. 71] gives an extraordinary way to test whether a curve is algebraic: Curve C is algebraic if and only if there exists a rational morphism $\phi : C \to \mathbb{P}^1$ which is ramified over only $\{0,1,\infty\}$. We shall not use his result, but rather an observation that is (a simple modification of) part of his proof:

Lemma 2. (Belyi[1]) *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 $\phi(S) \subset \{0,1,\infty\}$.*

This useful lemma is proved, for instance, by Serre as Theorem B on page 71 of [21] (for variations, see Belyi [1], Elkies [3], Langevin [16, 17], or my own less geometric account in [12]).

Assuming Lemma 2 we now proceed to the proof of Lemma 1. Let $S = \{(\alpha,\beta) \in \mathbb{P}^1 : f(\alpha,\beta) = 0\}$ and apply Lemma 2, writing $\phi(x/y) = a(x,y)/c(x,y)$, where $a(x,y), c(x,y) \in \mathbb{Q}[x,y]$ are homogenous forms, with 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 $t \in \mathbb{P}^1(\overline{\mathbb{Q}})$ 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 $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, we note (since $\mathbb{P}^1$ has genus zero, and ϕ is ramified only over $\{0,1,\infty\}$) that

$$2D = 2 + \sum_{u \in \{0,1,\infty\}} \left\{ D -^{\#} \phi^{-1}(u) \right\},$$

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

3. Proof of Theorem 5.

In [3] (around (26)), Elkies notes that his methods allow him to deduce, from the *abc*-conjecture, that Vojta's conjectured K-analogue of the Second Main Theorem of Nevanlinna theory is true for every number field K. Theorem 5 is just the case $K = \mathbb{Q}$; though the general case requires no further significant ideas. This same circle of ideas, with similar conclusions, appear in a paper of Langevin [17].

We deduce Theorem 5 from Lemma 1 as follows: Apply Lemma 1 and multiply together the distinct irreducible factors of $a(x,y)b(x,y)c(x,y)$ to we get a polynomial $f(x,y)g(x,y)$ of degree $D+2$.

Let $k = \gcd(a(m,n), b(m,n))$ where $(m,n) = 1$. It is easy to show that k divides the resultant of a and b, which is a non-zero integer, so that k is bounded. Now we apply the *abc*-conjecture directly to the equation $a/k + b/k = c/k$ to get

$$\max\{|a(m,n)|, |b(m,n)|\}^{1-\varepsilon} \ll \prod_{p|abc} p \ll \prod_{p|fg} p \le g(m,n) \prod_{p|f(m,n)} p.$$

Write $H = H(m,n) = \max\{|m|, |n|\}$. Note that if α is fixed then $|m - \alpha n| \ll H$. Thus $|g(m,n)| \ll H^{D+2-\deg(f)}$. Moreover, suppose that $\alpha \ne \beta$ are fixed. Since $(m-\alpha n)-(m-\beta n) = (\alpha-\beta)n$, and $\alpha(m-\beta n)-\beta(m-\alpha n)- = (\alpha-\beta)m$, we deduce that $\max\{|m-\alpha n|, |m-\beta n|\} \gg H$. Thus, since $a(x,y), b(x,y)$ have no common factors, $\max\{|a(m,n)|, |b(m,n)|\} \gg H^D$. The result follows from substituting these two estimates into the equation above.

4. Proofs of Theorems 1 and 2.

We begin by proving, in the notation of the Theorems:

Proposition 1. *There are $\sim c_f N$ positive integers $n \le N$ for which $f(n)/B'$ is not divisible by the square of a prime $p \le N$.*

Proposition 2. *There are $\sim c'_f MN$ pairs of positive integers $m \le M$, $n \le N$ for which $f(m,n)/B'$ is not divisible by the square of a prime $p \le \max\{M, N\}$.*

We describe here the proof of Proposition 1; the proof of Proposition 2 is mostly analogous and we will comment after, only on where the proofs significantly diverge.

To say that f/B' is squarefree means that it is not divisible by the square of any prime p. Thus, in Theorem 1, the number of $n \le N$ for which $f(n)/B'$ is squarefree is equal to the number of $n \le N$ for which $f(n)/B'$ is not divisible by the square of a prime $p \le z$, plus an error term bounded by the sum, over all primes $p > z$, of the number of integers $n \le N$ for which $f(n)/B'$ is divisible by p^2.

Now, if prime p does not divide either B or the discriminant of f, then $\omega_f(p) \le d :=$degree(f). We will select z larger than $B\text{disc}(f)$, so that

$$\sum_{p>z} \frac{\omega_f(p)}{p^{2+q_p}} \le d \sum_{p>z} \frac{1}{p^2} \ll \frac{1}{z}. \tag{3}$$

Selecting $z = \frac{1}{3}\log N$, we let $M = \prod_{p\le z} p^{2+q_p}$; by the prime number theorem $M = N^{2/3+o(1)}$. By the Chinese Remainder Theorem, there are exactly $M\prod_{p\le z}\left(1 - \frac{\omega_f(p)}{p^{2+q_p}}\right)$ integers n in any interval $(x, x+M]$, for which $f(n)/B'$ is not divisible by the square of a prime $p \le z$. Thus there are

$$\{N + O(M)\} \prod_{p\le z}\left(1 - \frac{\omega_f(p)}{p^{2+q_p}}\right)$$

integers $n \le N$ for which $f(n)/B'$ is not divisible by the square of a prime $p \le z$. By (3) we know that $c_f / \prod_{p\le z}\left(1 - \frac{\omega_f(p)}{p^{2+q_p}}\right) = 1 + O\left(\frac{1}{z}\right)$, and so we have proved

that there are $\sim c_f N$ integers $n \le N$ for which $f(n)/B'$ is not divisible by the square of a prime $p \le z$.

Now, there are $\omega_f(p)\{N/p^{2+q_p} + O(1)\}$ integers $n \le N$ for which $f(n)/B'$ is divisible by p^2, for any given prime p. If $p > z$ then this number is $\le dN/p^2 + O(d)$. Therefore the number of integers $n \le N$ for which $f(n)/B'$ is divisible by p^2, for some prime p in the range $z < p \le N$ is

$$\ll_d \sum_{z<p\le N} \left(\frac{N}{p^2} + 1\right) \ll \frac{N}{z} + \frac{N}{\log N} = o(N).$$

We have therefore proved Proposition 1.

To prove Proposition 2, suppose that $N \ge M$ (the $M > N$ case is handled analogously). Dealing with the primes $p \le z$ is done entirely analogously: the use of $\omega'_f(p)$, as opposed to $\omega_f(p)$, takes account of the slight differences in these cases. For the primes $p > z$, we first remove all pairs (m, n) which have a common prime factor $> z$. The number of such pairs is $\le \sum_{p>z} MN/p^2 \ll MN/z = o(MN)$.

Then we use the same argument as was used above for each $f(m, n)$, where m is fixed $\le M$. We have to be a little careful because the discriminant of $f(m, x)$ may be divisible by some primes which do not divide the discriminant of $f(1, x)$, but all of these primes will divide m. However, for such primes p, we note that p^2 divides $f(m, n)$ if and only if p divides some non-zero coefficient of f (note that p does not divide n, since it already divides m). However this is a finite set of primes, bounded independently of m, and thus the above estimates are uniform. Proposition 2 follows.

Now Propositions 1 and 2 are proved, we can complete the proof of Theorems 1 and 2 by showing that, for any fixed $\varepsilon > 0$, there are $O(\varepsilon N)$ integers $n \le N$ for which $f(n)$ is divisible by the square of a prime $> N$; and similarly that there are $O(\varepsilon MN)$ integers $m \le M$, $n \le N$ for which $f(m, n)$ is divisible by the square of a prime $> \max\{M, N\}$. Observe that such results are true for f if they are true for all of the irreducible factors of f; thus we will prove such a result assuming that f is irreducible over $\mathbb{Z}[x]$ (or $\mathbb{Z}[x, y]$, respectively). Now the square, of any prime $p > N$, is $> N^2$, so certainly cannot divide a non-zero value $|f(n)|$ of a linear polynomial f (since it is a lot bigger). In fact, we can alter the proofs of Propositions 1 and 2 to make the conclusions true with all primes $p \le cN$ (or $p \le c \max\{M, N\}$, respectively): choosing c large enough implies that the square of any prime $p > cN$ is greater than $|f(n)|$ (or $|f(m, n)|$, respectively) if f is quadratic. Thus Theorems 1 and 2 follow from the following result (taking $N = 1$ to prove Theorem 1):

Theorem 8. *Assume that the abc-conjecture is true. Suppose that $f(x, y) \in \mathbb{Z}[x, y]$ is homogenous and irreducible, of degree $d \ge 3$. Fix $\varepsilon > 0$. There are $O(\varepsilon MN)$ pairs of integers m and n, such that $f(m, n)$ is divisible by the square of a prime $> \max\{M, N\}$.*

In Theorem 6 we noted that $f(m, n)$ is not divisible by the square of any integer $> \max\{M, N\}^{2+\varepsilon}$. This is not quite enough to deduce Theorem 8, since we need to also rule out slightly smaller primes; that is, as small as $\max\{M, N\}$. Instead

we will apply Theorem 6 to a new polynomial,

$$F(x,y) := f(x,y)f(x+y,y)f(x+2y,y)\dots f(x+(k-1)y,y). \tag{4}$$

$F(x,y)$ has no repeated factors, for if it did then we would have roots α, β of $f(x,1)=0$, with $\beta = \alpha + i$ for some positive integer i. Since f is irreducible, the Galois group G for its splitting field extension is transitive and, so for any root γ of $f(\gamma,1)=0$ there exists $\sigma \in G$ for which $\gamma = \alpha^\sigma$. Select that root γ of $f(x,1)=0$ for which $\mathrm{Re}(\gamma)$ is maximal. Then $\beta^\sigma = \alpha^\sigma + i = \gamma + i$, so $\mathrm{Re}(\beta^\sigma) = \mathrm{Re}(\gamma) + i > \mathrm{Re}(\gamma)$, giving a contradiction.

Assume, for convenience, that $M > N$. Now, for every $m' \le M, n \le N$ with $(m',n)=1$, there exists some integer $m \in \mathcal{M}$ such that $m' = m + in$ for some $0 \le i < k$, where $\mathcal{M}$ is the set of integers m of the form $m = i + jnk$, where $0 < i < n$, $(i,n)=1$, $0 \le j \le [M/nk]$. Theorem 5 applied to $F(m,n)$ for each $m \in \mathcal{M}, n \le N$ implies[5] that there are at most two $f(m+in,n)$, $0 \le i < k$, which are divisible by the squares of primes $> M$. Thus, in total, there are $O(|\mathcal{M}|) = O(N^2 + MN/k)$ pairs $m' \le M, n' \le N$, $(m',n')=1$, such that $f(m',n')$ is divisible by the square of a prime $> M$. Selecting $k = [1/\varepsilon]$ implies Theorem 8, provided $N = O(\varepsilon M)$.

We would like to apply a similar argument to deduce Theorem 8 when $M = O(N)$. Let us suppose that we can find some finite set $\mathcal{T}$ of "distinct"[6] matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$; such that for any sufficiently large $R := \max\{M,N\}$, there exists a set $\mathcal{L}$ of $O(\varepsilon^2 R^2)$ lattice points such that

$$\{(x,y) \in \mathbb{Z}^2 : \ 1 \le x,y \le R, (x,y)=1\} \subset \bigcup_{(m,n)\in\mathcal{L}} \{(am+bn, cm+dn) : \ A \in \mathcal{T}\}.$$

Let

$$F(x,y) := \prod_{A\in\mathcal{T}} f(A\underline{x}) \qquad \text{where} \quad A\underline{x} := (ax+by, cx+dy).$$

A priori we have no reason to believe that we can apply Theorem 5 to $F(x,y)$, since it may have repeated roots. In the Appendix we show that, since $\deg(f) > 2$, there is a group H of at most 12 matrices, such that if $f(\underline{x})$ and $f(A\underline{x})$ have common roots then $A \in H$. Let $\mathcal{T}'$ be a subset of the matrices in $\mathcal{T}$, constructed by selecting exactly one matrix from each orbit $\{hA : \ h \in H\}_{A\in\mathcal{T}}$. Then we can apply Theorem 5 to $G(x,y) := \prod_{A\in\mathcal{T}'} f(A\underline{x})$, for each $(x,y) \in \mathcal{L}$. Proceeding as before we now have at most $2 \times 12 \times |\mathcal{L}| = O(\varepsilon^2 R^2) = O(\varepsilon MN)$ pairs $1 \le m,n \le R$ with $(m,n)=1$, for which $f(m,n)$ is divisible by the square of a prime $> R$, and we have thus proved Theorem 8.

[5] Note that if q^2 divides $f(m,n)$, where $q > M$, then $\prod_{p|f(m,n)} p \ll M^{\deg(f)-1}$. Thus if three of the $f(m+in,n)$ were divisible by squares of primes $> M$, we'd have $\prod_{p|F(m,n)} p \ll M^{\deg(F)-3}$ contradicting Theorem 5.

[6] We take $\gcd(a,b,c,d)=1$, without loss of generality, and thus ensure that the matrices are distinct in $\mathrm{PGL}(2,\mathbb{Z})$.

It only remains to show that we can construct such a set $\mathcal{T}$, and the set $\mathcal{L}$ of lattice points for any given R: We define

$$\mathcal{L} := [1, \varepsilon R] \times [1, \varepsilon R] \quad \bigcup \quad [1, \varepsilon^2 R] \times [1, R] \quad \bigcup \quad [1, R] \times [1, \varepsilon^2 R],$$

and $\mathcal{T}$ to be the set of all "free words"[7] of length $\le [2/\varepsilon^2]$ on the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. We need to show that for every $(x, y) \in [1, R] \times [1, R]$, where the $\gcd(x, y) = 1$, there is some $A \in \mathcal{T}$, such that $A^{-1}(x, y) \in \mathcal{L}$. We will construct A^{-1}, which will be a free word of length $\le [2/\varepsilon^2]$ on $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. We now describe our algorithm to construct A^{-1}:

Take $A = I$ for all $(x, y) \in \mathcal{L}$. Otherwise, we may assume $x, y > \varepsilon^2 R$. The matrices correspond to the transformations $(x, y) \to (x-y, y)$ and $(x, y) \to (x, y-x)$ (note that both maps keep $\gcd(x, y) = 1$ fixed). We select the first map if $x > y$, the latter map if $x < y$ (note $x = y$ implies we have the point $(1, 1)$). The new lattice point is also inside the top right quadrant, and the sum of its ordinates has been reduced by at least $\varepsilon^2 R$. We repeat this process until the transformed lattice point is in $\mathcal{L}$. This must happen within $[2/\varepsilon^2]$ iterations of our algorithm, else the transformed lattice point is still in the top right quadrant, and the sum of its ordinates is $\le R + R - [2/\varepsilon^2]\varepsilon^2 R < \varepsilon^2 R$, which means that it is in $\mathcal{L}$.

5. Proof of Theorem 3, assuming Theorem 6.

We proceed much as in the previous section: Let $k = [9/\varepsilon]$ and define $g(t) = (t+1)(t+2)(t+3)\dots(t+k)$.

Using the sieve of Eratosthenes one knows that there are $\sim \frac{6}{\pi^2} x^\varepsilon < \frac{2}{3} x^\varepsilon$ integers in the interval $(x, x + x^\varepsilon)$ which are not divisible by the square of a prime $\le x^\varepsilon$. Thus, if there are to be no squarefree integers in this interval, then there must be at least $\frac{1}{3} x^\varepsilon$ integers $m \in (x, x + x^\varepsilon)$ divisible by the square of a prime $> x^\varepsilon$. But that means there is an integer $m \in (x, x + x^\varepsilon)$ such that at least one-quarter of the integers $(m+1), (m+2), \dots, (m+k)$ are divisible by the square of a prime $> x^\varepsilon$. Thus $g(m)$ is divisible by the square of an integer $> (x^\varepsilon)^{k/4} > m^2$ contradicting Theorem 6.

6. Proof of Theorem 4.

As we noted in the introduction Theorem 4 follows once we prove (2), which we will now do. By adjusting the constant in (2) as necessary, we can assume that T is sufficiently large. By Theorem 3, we know that $S(x; t) = 0$ when $t \gg x^\varepsilon$; In particular when $t \ge x^{1/2A(A+1)}$ and x is sufficiently large. Thus we will prove (2) assuming that $2(A+2)^2 < T < x^{1/2A(A+1)}$. Let B be the smallest integer $\ge A$.

We begin by noting that, by the sieve of Eratosthenes, there are $\ge (3/5)t$ integers in any interval of length $t \ge T$, which are not divisible by the square of any prime $\le 2T$ (note that $3/5 < 6/\pi^2$).

[7] That is, all expressions of the form $XXYYYXYYYXXX\dots XY$, with the Xs and Ys in any order

Let $S'(x;T)$ count the number of $s_n \le x$ with $T \le s_{n+1} - s_n < 2T$, for which there are $\ge T/2$ integers in the interval (s_n, s_{n+1}) which are not divisible by the square of any prime $\le 2T$ or $> T^A$. Note that for any $s_n \le x$ counted by $\sum_{T \le t < 2T} S(x;t)$ but not by $S'(x;T)$, there must be $> T/10$ integers $m \in (s_n, s_{n+1})$ which are divisible by the square of some prime $> T^A$. Therefore

$$\frac{T}{10}\left(\sum_{T\le t<2T} S(x;t) - S'(x;T)\right) \le \sum_{\substack{m\le x \\ p^2|m \text{ for some } p>T^A}} 1$$
$$\le \sum_{p>T^A} \sum_{m\le x,\ p^2|m} 1 \le \sum_{p>T^A} \frac{x}{p^2} \ll \frac{x}{T^A}.$$

This contribution to the sum in (2) is acceptably small.

If s_n is counted by $S'(x;T)$ then there are $\ge T/2$ integers in the interval (s_n, s_{n+1}) divisible by the square of a prime in the range $[2T, T^A]$. Thus there are at least $\binom{[T/2]}{B}$ different B-tuples of integers of the form

$$s_n < k_1 p_1^2 < k_2 p_2^2 < \cdots < k_B p_B^2 < s_{n+1}$$

with the p_j are distinct primes from $[2T, T^A]$. Note that we can write $k_j p_j^2 = k_1 p_1^2 + d_j$ for $2 \le j \le B$ where $1 \le d_2 < d_3 < \cdots < d_B \le 2T$. Taking together all such B-tuples from all of the s_n counted by $S'(x;T)$, we get

$$S'(x;T)\binom{[T/2]}{B} \le \sum_{\substack{2T<p_1,p_2,\dots,p_B<T^A \\ p_j \text{ distinct}}} \sum_{1\le d_2<d_3<\cdots<d_B\le 2T} \sum_{\substack{k_1p_1^2\le x \\ k_jp_j^2=k_1p_1^2+d_j \text{ for } 2\le j\le B}} 1.$$

Let's concentrate on the last sum first. If we let $r = k_1 p_1^2$, then we see that $r \equiv 0 \pmod{p_1^2}$, and $r \equiv -d_j \pmod{p_j^2}$ for $2 \le j \le B$. Thus r is in some fixed residue class $r_0 \pmod{(p_1 p_2 \dots p_B)^2}$. There are $\le x/(p_1 p_2 \dots p_B)^2 + 1$ such integers $r \le x$; and this quantity is $\le 2x/(p_1 p_2 \dots p_B)^2$ since $(p_1 p_2 \dots p_B)^2 \le T^{2AB} < T^{2A(A+1)} < x$. Noting also that there are precisely $\binom{2T}{B-1}$ choices for the d_j in the sum above, we get

$$S'(x;T)T^B \ll_B \sum_{2T<p_1,p_2,\dots,p_B<T^A} \binom{2T}{B-1} \frac{2x}{(p_1p_2\dots p_B)^2}$$
$$\ll xT^{B-1}\left(\sum_{p\ge 2T} \frac{1}{p^2}\right)^B \ll \frac{x}{T}$$

which implies (2).

Appendix: Fractional linear transformations of roots of an irreducible polynomial.[8]

Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $d \geq 2$. We wish to determine all fractional linear transformations (that is elements of $\mathrm{PGL}(2,\mathbb{Q})$), which send some root of f to some other root of f.

All such transformations are of the form $\beta = \frac{a\alpha+b}{c\alpha+d}$, with $a, b, c, d \in \mathbb{Z}$. Applying any element σ of the Galois group gives $\beta^\sigma = \frac{a\alpha^\sigma+b}{c\alpha^\sigma+d}$. Since the Galois group, G, is transitive, the action of the linear transformation defines a permutation of all of the roots of f. Since we can compose permutations, we see that our transformations form a group, call it $H = H_f$.

Quadratic polynomials: $d = 2$:

Make a change of variable of the form $x \to x + a$ to guarantee that $f(x)$ is of the form $x^2 - m$ where m is not a square[9]. Such a transformation which sends $\sqrt{m} \to \pm\sqrt{m}$ gives

$$\frac{a\sqrt{m}+b}{c\sqrt{m}+d} = \pm\sqrt{m}.$$

Multiplying through by the denominator, we obtain $a\sqrt{m} + b = \pm(cm + d\sqrt{m})$ so that $b = \pm cm$ and $a = \pm d$. Thus the set of such transformations are given by the matrices

$$\begin{pmatrix} \pm d & \pm cm \\ c & d \end{pmatrix}, \qquad (c,d) \in \mathbb{P}^1(\mathbb{Q}).$$

H is isomorphic to the group (under multiplication) $\{d + c\sqrt{m}\}/\mathbb{Q}^*$ with $c, d \in \mathbb{Q}$; and thus has infinite rank.

Higher degree polynomials: $d \geq 3$:

Suppose now that $(a\alpha + b)/(c\alpha + d) = \alpha$ where α is a root of f. Then $c\alpha^2 + (d-a)\alpha - b = 0$. But α is a root of an irreducible polynomial of degree > 2, so we must have $c = a - d = b = 0$, that is our linear transformation is the identity map (as a matrix it is the identity in $\mathrm{PGL}(2,\mathbb{Q})$).

Now if $A \in H$ each $A^r\alpha$ gives a root of f; and since there are d different roots we must have $A^r\alpha = A^s\alpha$ $(= \beta$, say) for some $0 \leq r < s \leq d$. Therefore $A^n\beta = \beta$ where $n = s - r$, and so A^n is the identity map by what we proved in the paragraph above. In particular we see that A is invertible.

If $A, B \in H$ and $A\alpha = B\alpha$ $(= \beta$, say) then $AB^{-1}\beta = \beta$, so AB^{-1} is the identity, so $A = B$. Therefore, since the $A\alpha$ must be distinct, H can have no more than d elements. Thus we see that H is a finite subgroup of $\mathrm{PGL}(2,\mathbb{Q})$; all such subgroups can be identified:

[8]Special thanks to Dan Abramovich and Jean-Pierre Serre for their observations included below. I would also like to thank Malcolm Adams, Dave Benson, Elham Izadi, Will Kazez, Dino Lorenzini, Robert Rumely and Ted Shifrin for useful conversations pertaining to this section.

[9]Note that the transformation $x \to x + a$ is itself a fractional linear transformation, so we do this without any loss of generality, since we can compose such transformations.

Proposition A. *The finite subgroups of $PGL(2,\mathbb{Q})$ are precisely $1, C_2, C_3, C_4, C_6$, $D_{2\times 2}, D_{2\times 3}, D_{2\times 4}$ and $D_{2\times 6}$.*

All the groups listed in Proposition A do occur as subgroups of $\mathrm{PGL}(2,\mathbb{Q})$. Explicitly $D_{2\times n} := \{A_n^n = B^2 = I : \ A_nBA_n = B\}$ where $B : z \to 1/z$, and C_n is generated by A_n, where

$$A_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \ A_3 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \ A_4 = \begin{pmatrix} 1 & 5 \\ -5 & 7 \end{pmatrix}, \text{ and } A_6 = \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}.$$

Realizing the finite subgroups of $PGL(2,\mathbb{Q})$ as H_f

Note that $H_f = C_1$ for $f(z) = z^3 - 2$, and $H_f = C_2$ for $f(z) = z^4 - 2$, where the element in C_2 of order 2 is given by the involution $z \to -z$. It is easy to construct examples when $|H| = 1$ or 2, by any *ad hoc* method.

Given one of the groups H in Proposition A, of order at least 3, can we find polynomials f with $H_f = H$? Dan Abramovich pointed out to me that if we have a rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1/H$, and we take a set S of roots of some given polynomial g, then, in all but finitely many cases, $\phi^{-1}(S)$ will be the set of roots of some polynomial f with $\deg f = |H| \deg g$. An argument can be made that "typically" if g is irreducible then f will also be irreducible[10]. It is easy enough to make Abramovich's idea concrete in our finitely many cases, to find examples of irreducible f of degree $|H|$ with $H_f = H$, when $|H| \geq 3$:

In order to force f to be irreducible of degree $|H|$, we take S to contain one element. We wish to write ϕ as an invariant rational function of degree $|H|$; the obvious function to try is the trace, $\phi(z) := \sum_{h\in H} hz$. This usually worked, though occasionally there was some cancellation between terms[11], in which case we instead used $\phi(z) := \sum_{h\in H}(hz)^2$ (whether there is such cancellation depends on which particular explicit representation of H in $\mathrm{PGL}(2,\mathbb{Q})$ one uses in the calculations).

For the cyclic group $H = C_n$, we write $\phi(z) = u(z)/cv(z) := \sum_{h\in H} hz$ where u and v are monic without common roots, and c is a constant. Evidently the roots of $f(z) = u(z) - jv(z)$ are permuted by H, and $u(z) - jv(z)$ is irreducible for "almost all" j, by Hilbert's Irreducibility Theorem. Thus if C_n is generated by M_n then we get f_n, as below:

$$M_3 := \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \quad M_4 := \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \text{ and } \quad M_6 := \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}$$

with

$$f_3(z) = (z^3 - 3z - 1) - jz(z+1),$$
$$f_4(z) = (z^2 - 2z - 1)(z^2 + 2z - 1) - j(z^3 - z), \quad \text{and}$$
$$f_6(z) = (z^3 + 3z^2 - 1)(z^3 - 3z^2 - 6z - 1) - j(z-1)z(z+1)(z+2)(2z+1).$$

[10] And "typically" can be made more precise via the Hilbert Irreducibility Theorem.

[11] For example, if the map $z \to -z$ is in H then $\sum_{h\in H} hz = 0$.

We followed the same strategy with $D_{2\times 4}$ (generated by B and A_4 as above), to obtain

$$f_{2\times 4} := 175 + 2900z^2 - 16320z^3 + 26746z^4 - 16320z^5 + 2900z^6 + 175z^8 \\ - jz(z+5)(3z-5)(5z+1)(5z-3)(5z-7)(7z-5).$$

For the other dihedral groups we found that there was cancellation in $\sum_{h\in H} hz$, and so we had to replace it in the above computations by $\sum_{h\in H}(hz)^2$ — this worked on the three remaining occasions, and we obtained

$$f_{2\times 2}(z) = z^4 + 1 - jz^2,$$
$$f_{2\times 3}(z) = (z^2 - z + 1)^3 - jz^2(z-1)^2, \quad \text{and}$$
$$f_{2\times 6}(z) = 4 + 24z + 72z^2 + 140z^3 + 285z^4 + 564z^5 + 738z^6 + 564z^7 + 285z^8 \\ + 140z^9 + 72z^{10} + 24z^{11} + 4z^{12} - j((z-1)z(z+1)(z+2)(2z+1))^2.$$

(The class of polynomials $f_{2\times 3}(z)$ are familiar from the construction of the λ-invariant of elliptic curves out of the j-invariant.)

The finite subgroups of $PGL(2,\mathbb{Q})$: Proofs

To prove that no groups H can occur, other than those listed in Proposition A, we use Serre's result ([20], Proposition 16) that if H is a finite subgroup of $\mathrm{PGL}(2,k)$, where k is a field whose characteristic is coprime with the order of H, then the only possibilities for H are the cyclic groups C_n, the dihedral groups $D_{2\times n}$, the alternating groups A_4 or A_5, and the symmetric group S_4. Moreover he remarks on the same page that if the characteristic of k is not 2 then A_4 and S_4 are subgroups of $\mathrm{PGL}(2,k)$ if and only if -1 is the sum of two squares in k; and A_5 is a subgroup of $\mathrm{PGL}(2,k)$ if and only if, in addition, -5 is a square in k.

Thus we note that none of A_4, A_5, S_4 are subgroups of $\mathrm{PGL}(2,\mathbb{Q})$, or even $\mathrm{PGL}(2,\mathbb{R})$, by Serre's criterion. We are therefore left with the cyclic and dihedral groups. To complete the proof of Proposition A we will prove the following:

Lemma A1. *If matrix A has finite order n in $PGL(2,\mathbb{Q})$ then $n = 1, 2, 3, 4$ or 6.*

Proof of Lemma A1. A matrix A of finite order n in $\mathrm{PGL}(2,\mathbb{Q}) = \mathrm{PGL}(2,\mathbb{Z})$ satisfies an equation $A^n = \lambda I$, with $\lambda \in \mathbb{Z}$, as well as the quadratic equation $A^2 - TA + D = 0$, where T =Trace(A) and D =Determinant(A) are both integers. Thus the minimal polynomial, $m(x)$, for A divides both $x^2 - Tx + D$ and $x^n - \lambda$.

If $m(x)$ has degree 1 then $A = I$ in $\mathrm{PGL}(2,\mathbb{Q})$, so that $n = 1$ and $T^2 = 4D$.

So now assume that $m(x)$ has degree ≥ 2; since it divides $x^2 - Tx + D$, we must have $m(x) = x^2 - Tx + D$ divides $x^n - \lambda$. Thus the roots of $m(x)$ are distinct (since the roots of $x^n - \lambda$ are distinct). We see that $n = 2$ if and only if $T = 0$.

So now assume $n \geq 3$ so that $T \neq 0$. Let $\rho = |\lambda|^{1/n}$. The roots of $x^2 - Tx + D$ must be of the form $\zeta\rho$ and $\xi\rho$, where where ζ and ξ are $2n$th roots of unity. Then $\zeta + \xi = T/\rho \neq 0$ is real, and so $\xi = \overline{\zeta}$. Therefore $D = \rho^2$ and thus $\zeta^2 + \overline{\zeta}^2 = T^2/D - 2$. The left side of this equation gives that this is an algebraic integer, the right side that it is rational, and so it must be a rational integer. Since $|\zeta^2 + \overline{\zeta}^2| \leq 2$, we see that the integer must be $-2, -1, 0, 1$ or 2, and thus $T = 0$ or $T^2 = D, 2D, 3D$ or

$4D$. These leads to the three cases x^2+x+1 divides x^3-1, and $x^2+x+1/2$ divides $x^4+1/4$, and $x^2+x+1/3$ divides $x^6+1/27$, so that we can have $n=3,4$ or 6, respectively. In fact we have proved slightly more than previously claimed:

Lemma A1'. *If A has finite order n in $PGL(2,\mathbb{Q})$ then $D=$Determinant$(A)\neq 0$. In fact, for $T=$Trace(A) we have $n=1$ iff $T^2=4D$; $n=2$ iff $T=0$; $n=3$ iff $T^2=D$; $n=4$ iff $T^2=2D$; and $n=6$ iff $T^2=3D$.*

Remark. In an 7/4/98 email correspondence, Serre remarks that C_n and $D_{2\times n}$ are subgroups of $\mathrm{PGL}(2,k)$, where k is a field of characteristic 0, if and only if $\zeta+\overline{\zeta}\in k$, where ζ is a primitive nth root of unity. Note that, by combining this with Serre's results from [20], Proposition A follows as an immediate consequence.

To prove this for C_n, Serre improves on our proof of Lemma A1, obtaining his criterion by noting that $T^2/D=z+\overline{z}+2$, where z is actually a primitive nth root of unity. He then extends this to $D_{2\times n}$ by showing, via an explicit matrix construction, that if A represents a semisimple element of $\mathrm{PGL}(2,k)$ then there is an inner automorphism of that group, of order 2, which transforms A to its inverse.

An observation

Note that any linear transformation $A\in\mathrm{PGL}(2,\mathbb{Q})$ and any field automorphism σ obviously commute. Thus if there is some $\sigma\in G$ and $A\in H$ which have the same "action" on the roots of f (that is, $A\alpha=\sigma\alpha$ for all roots α), then σ must lie in the center of G, and A in the center of H. Of the groups listed in Proposition A, $1, C_2, C_3, C_4, C_6, D_{2\times 2}$ are all commutative, $D_{2\times 3}$ has trivial center, and $D_{2\times 4}$ and $D_{2\times 6}$ have center C_2.

References

[1] G.V. Belyi, *On the Galois extensions of the maximal cyclotomic field (in Russian)*, Izv. Akad. Nauk SSSR. **43** (1979), 267-276.

[2] 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.

[3] N. Elkies, *ABC implies Mordell*, Int. Math. Res. Not. **7** (1991), 99-109.

[4] P. Erdős, *Some problems and results in elementary number theory*, Publ. Math. Debrecen **2** (1951), 103-109.

[5] P. Erdős, *Arithmetical Properties of Polynomials*, J. London Math. Soc. **28** (1953), 416-425.

[6] P. Erdős, *Problems and results on consecutive integers*, Publ. Math. Debrecen **23** (1976), 271-282.

[7] J.-H. Evertse and J.H. Silverman, *Uniform upper bounds on the number of solutions to $Y^n=f(X)$*, Math. Proc. Camb. Phil. Soc. **100** (1986), 237-248.

[8] M. Filaseta, *On the distribution of gaps between squarefree numbers*, Mathematika **40** (1993), 88101.

[9] M. Filaseta and O. Trifonov, *On gaps between squarefree numbers II*, J. London Math. Soc. **45** (1992), 215-221.

[10] 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.

[11] A. Granville, *On the scarcity of powerful binomial coefficients* (to appear).

[12] A. Granville, *It's as easy as abc* (to appear).

[13] G. Greaves, *Power-free values of binary forms*, Quart. J. Math. Oxford **43** (1992), 45-65.

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

[15] C. Hooley, *On the distribution of square-free numbers*, Can. J. Math. **25** (1973), 1216-1223.

[16] M. Langevin, *Cas d'égalité pour le théorème de Mason et applications de la conjecture (abc)*, C. R. Acad. Sci. Paris **317** (1993), 441-444.
[17] M. Langevin, *Partie sans facteur carré de $F(a,b)$ (modulo la conjecture (abc))*, Séminaire de Théorie des Nombres, Publ. Math. Univ. Caen (1993–94).
[18] M. Ram Murty, *The ABC Conjecture and exponents of quadratic fields*, Contemp. Math **210** (1997), 85-95.
[19] M. Ram Murty, *Exponents of class groups of quadratic fields* (to appear).
[20] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math **15** (1972), 259-331.
[21] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, Viewig, Braunschweig, 1990.
[22] P. Vojta, *Diophantine Approximations and Value Distribution Theory*, Lecture Notes in Math. **1239** (1987).

Department of Mathematics, University of Georgia, Athens, Georgia 30602, USA
E-mail address: andrew@math.uga.edu