RATIONAL AND INTEGRAL POINTS ON QUADRATIC TWISTS OF A GIVEN HYPERELLIPTIC CURVE

Andrew Granville

Abstract. We show that the *abc*-conjecture implies that few quadratic twists of a given hyperelliptic curve have any non-trivial rational or integral points; and indicate how these considerations dovetail with other predictions.

1. Introduction.

For a curve C of genus $g > 1$, and number field K, Faltings' theorem implies that there are only finitely many K-rational points on C; that is $C(K)$ is finite. Moreover, assuming the Bombieri-Lang conjecture for rational points on surfaces of general type, Caporaso, Harris and Mazur [4] showed that $\#C(K) \ll_{g,K} 1$, where this bound is independent of C; further, they deduced that $\#C(K) \ll_g 1$ for all but $O_{g,K}(1)$ curves C defined over K.

Elkies [10] re-proved Faltings' theorem assuming the *abc*-conjecture, the advantage of his proof being that it gives a bound on the height of rational points on C. However, to determine this bound one needs to determine a "Belyi map" from C to $\mathbb{P}^1$ and the bounds thus obtained seem to be large compared to what one might suppose is true.

We believe that there are no non-trivial rational points on most curves of genus $g > 1$, an expectation into which the above proofs do not seem to give insight. The main purpose of these notes is to speculate on how often curves of genus $g > 1$ have no non-trivial rational points in a specific case of interest, and to prove results assuming the *abc*-conjecture.

Hyperelliptic curves of genus g, defined over the rationals, can be put in the form

$$C: \ y^2 = f(x)$$

where $f(x)$ is a polynomial with integer coefficients of degree $2g + 2$ or $2g + 1$, which has no repeated roots. The dth quadratic twist of C is the hyperelliptic curve

$$C_d: \ d\,y^2 = f(x).$$

We remind the reader of

Typeset by $\mathcal{AMS}$-TEX

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

$$c \ll N(abc)^{1+o(1)},$$

where $N(m)$ is the product of the distinct primes dividing m (that is, $N(\prod_p p^{e_p}) = \prod_p p$). (Here the "$o(1)$" term approaches 0 as $N(abc) \to \infty$ or, equivalently, $c \to \infty$.)

A *Belyi map* is a rational function from a given curve to $\mathbb{P}^1$ which ramifies over no more than three points. Belyi showed how to construct such a map from $\mathbb{P}^1$ to $\mathbb{P}^1$ whose critical points include any given finite set of points. So, for a hyperelliptic curve C, we can first map each point on the given curve to its x-coordinate and then compose this projection with our Belyi function from $\mathbb{P}^1$ to $\mathbb{P}^1$, where our given finite set of points includes the roots of f, as well as $x = \infty$ if the degree of f is odd, to obtain a Belyi map for the original curve. From this construction we see that we can take the same Belyi map from C_d to $\mathbb{P}^1$ for each d, that is the same rational function of the variable x only. Armed with this construction we apply the *abc*-conjecture as in Elkies' work [10], but now the *abc*-conjecture applies uniformly to the family of quadratic twists of the given hyperelliptic curve C, leading to the following bounds on the size of rational and integral points on the curves C_d.

Theorem 1. *Assume that the abc-conjecture is true. Suppose that $f(x) \in \mathbb{Z}[x]$ does not have repeated roots.*

(i) *If $g \geq 1$ then the integral points on C_d with x-coordinate r satisfy*

$$|r| \ll |d|^{1/(\deg(f)-2)+o(1)}.$$

(ii) *If $g \geq 2$ then the rational points on C_d with x-coordinate r/s where $(r, s) = 1$ satisfy*

$$|r|, |s| \ll |d|^{1/(2g-2)+o(1)}.$$

We believe that Theorem 1 is best possible in that there are integral (and rational) points on various C_d with such large x-coordinates, and we will prove this whenever f has a factor of degree two (a factor of degree four, respectively) over $\mathbb{Q}$.

Certain rational points predictably occur on each C_d, namely those with y-coordinate 0 as well as the points at ∞ when f has odd degree, and so are uninteresting for us. We call these the "trivial points". Our goal is to determine how many C_d possess other rational points, that is, "non-trivial points".

Since each value of r/s with $f(r/s) \neq 0$ gives rise to a unique squarefree d, we can immediately deduce the following result from Theorem 1.

Corollary 1. *Assume that the abc-conjecture is true. Suppose that $f(x) \in \mathbb{Z}[x]$ does not have repeated roots.*

(i) *If f has degree ≥ 3 (that is $g \geq 1$) then there are $\ll_f D^{1/(\deg(f)-2)+o(1)}$ squarefree integers d with $|d| \leq D$ for which C_d has a non-trivial integral point.*

(ii) *If f has degree ≥ 5 (that is $g \geq 2$) then there are $\ll_f D^{1/(g-1)+o(1)}$ squarefree integers d with $|d| \leq D$ for which C_d has a non-trivial rational point.*

Therefore there are $\ll_f D^{1/2+o(1)}$ values of $|d| \leq D$ for which C_d has a non-trivial rational point if $g \geq 3$ (assuming the *abc*-conjecture). We believe that Corollary 1 is not far from the best possible:

Conjecture 1. *If $f(x) \in \mathbb{Z}[x]$ does not have repeated roots then there exist constants $\kappa_f, \kappa'_f > 0$ for which*

(i) *There are $\sim \kappa_f D^{1/\deg(f)}$ squarefree integers d with $|d| \leq D$ for which C_d has a non-trivial integral point, provided deg$(f) \geq 3$.*

(ii) *There are $\sim \kappa'_f D^{1/(g+1)}$ squarefree integers d with $|d| \leq D$ for which C_d has a non-trivial rational point, provided $g \geq 2$.*

We will give (conjectural) values for κ_f and κ'_f below. The results in [12] can be used to deduce that the lower bounds implicit in Conjecture 1 hold (with the same constants κ_f and κ'_f), assuming the *abc*-conjecture. Stewart and Top [16, Theorem 2] came close to proving this, unconditionally, by showing that there are $\gg_f D^{1/(g+1)}/\log^2 D$ squarefree integers $d \leq D$ for which C_d has a non-trivial rational point. In fact, we can prove Conjecture 1 for a family of hyperelliptic curves, assuming the *abc*-conjecture:

Theorem 2. *Assume that the abc-conjecture is true, and suppose that $f(x) \in \mathbb{Z}[x]$ factors into distinct linear factors over $\mathbb{Q}$. If $f(x)$ has degree ≥ 7 (so that $g \geq 3$) then Conjecture 1(i) is true for f. If $f(x)$ has degree ≥ 25 (so that $g \geq 12$) then Conjecture 1(ii) is true for f.*

The work of Caporaso, Harris and Mazur discussed above suggests that the number of rational points on C_d is uniformly bounded. It is of interest to explicitly determine that bound, though some clarifications are necessary. Rational and integral points come in automorphism classes (that is, orbits of the action of the automorphism group). We always have the automorphism $(x, y) \mapsto (x, -y)$. There is sometimes also an automorphism $(x, y) \mapsto (a - x, \pm y)$ for some fixed integer a, for integral points; and sometimes automorphisms of the form

$$(x, y) \mapsto \left(\frac{\alpha x + \beta}{\gamma x + \delta}, \frac{\pm \eta y}{(\gamma x + \delta)^{g+1}} \right),$$

for some fixed integers $\alpha, \beta, \gamma, \delta, \eta$, for rational points. We denote by Aut(C) the (finite) group of such automorphisms of C, and define $c_d(\mathbb{Z})$ and $c_d(\mathbb{Q})$ to be the number of automorphism classes of non-trivial integral and rational points on C_d, respectively. We believe that these are typically small:

Conjecture 2. *There exists a constant g_0 such that if $f(x) \in \mathbb{Z}[x]$ does not have repeated roots and $g \geq g_0$ then*

(i) *There are only finitely many squarefree integers d for which $c_d(\mathbb{Z}) > 1$.*

(ii) *There are only finitely many squarefree integers d for which $c_d(\mathbb{Q}) > 2$.*

Remarks. One can easily find, by interpolation methods, a monic polynomial f of degree n such that $(x, f(x))$ passes through n given points. If these are all integral points then one usually has $c_1(\mathbb{Q}) \geq c_1(\mathbb{Z}) \geq n$. This does not contradict our conjecture since we have allowed for finitely many exceptional d.

Any curve of genus $g > 1$ has finitely many rational points. By multiplying the coefficients of f by appropriate powers of the least common multiple, L, of the denominators of these rational points, we obtain a model for the curve on which all the rational points are now integral. This can not be done simultaneously for all twists, as L will go to ∞. However it does mean that we cannot uniformly bound the "finitely many" in (i).

It is known that $\#\mathrm{Aut}(C) \leq 84(g-1)$; so our conjecture implies specific uniform bounds for the number of integral and rational points on the quadratic twists of a given hyperelliptic curve, with finitely many exceptions (that is, exceptional twists).

In Theorem 5(i) (in section 8) we exhibit certain infinite families of curves, C, for which Conjecture 2(i) is true, assuming the *abc*-conjecture. Moreover, in Theorem 5(ii), we exhibit certain infinite families of C for which there are only finitely many squarefree integers d with $c_d(\mathbb{Q}) > 1$ assuming the *abc* and *abcd* conjectures, that is, even more than Conjecture 2(ii) is true.

We can go further than Conjecture 2 assuming the

Bombieri-Lang conjecture. *Let X be any variety of general type, defined over a number field K. There exists a proper closed subvariety $S \subset X$ such that for any number field L containing K, the set of L-rational points of X lying outside of S is finite.*

Theorem 3. *Assume that the Bombieri-Lang conjecture is true. If $f(x) \in \mathbb{Z}[x]$ does not have repeated roots and $g > 1$ then the set of squarefree integers d for which $c_d(\mathbb{Q}) \geq 2$ may be parameterized by the rational points on a finite number of curves of genus 0 and 1, together with finitely many exceptional d.*

Here we use the Bombieri-Lang conjecture only for surfaces of the form $z^2 = g(x)g(y)$ where $g(X) \in \mathbb{Z}[X]$ has even degree ≥ 6.

Conjecture 2 and Theorem 3 suggest that quadratic twists with $c_d(\mathbb{Z}) > 1$ or $c_d(\mathbb{Q}) > 1$ are rare. We now give explicit bounds on this:

Theorem 4. (i) *Assume that the abc-conjecture is true. If $f(x) \in \mathbb{Z}[x]$ factors into distinct linear factors over $\mathbb{Q}$, with $g \geq 3$ then there are*

$$\ll D^{2/(3(\deg(f)-2))+o(1)}$$

squarefree integers $d \leq D$ for which $c_d(\mathbb{Z}) \geq 2$.

(ii) *Assume that the Bombieri-Lang conjecture and Conjecture 1(ii) are true. There are $\ll D^{1/(2g)}$ squarefree integers $d \leq D$ for which $c_d(\mathbb{Q}) \geq 2$.*

If we do not assume Conjecture 1(ii) in the hypothesis of Theorem 4(ii), but rather the *abc*-conjecture, then we only prove that there are $\ll D^{1/(2g-2)+o(1)}$ squarefree integers $d \leq D$ for which $c_d(\mathbb{Q}) \geq 2$.

We will show that Theorem 4(ii) is close to best possible by exhibiting, under the assumption of the *abc*-conjecture, infinite families of curves C for which there are $\gg_f D^{1/(2g+1)}$ squarefree integers $d \leq D$ with $c_d(\mathbb{Q}) \geq 2$.

In section 9 we make a couple of general remarks that arise from these considerations. Then, in section 10, we extrapolate these ideas to make predictions about quadratic twists containing infinitely many rational or integral points. Finally, in section 11, we extend some of our results to the quadratic twists of superelliptic curves.

Notation: Throughout $f(x)$ is a polynomial of degree n, with leading coefficient $f_0 \neq 0$, with all integer coefficients and no repeated roots. Here $n = 2g+1$ or $2g+2$, and we define $F(x,z) = z^{2g+2} f(x/z)$.

Define $V_f = 2|f_0|^{-1/n}$ and $A_f = 1$ or 2, equalling 2 if and only if there exists $\ell \in \mathbb{Z}$ such that $f(x) = f(\ell - x)$. For each integer r let $\omega(r)$ be the number of residue classes t (mod r) for which r divides $f(t)$. Then define $\kappa_f = \kappa_{f,2}$ where

$$\kappa_{f,m} := \frac{V_f}{A_f} \prod_p \left\{ 1 + \left(1 - \frac{1}{p^{m/n}}\right) \left(\frac{\omega(p^m)}{p^{m(1-1/n)}} + \frac{\omega(p^{2m})}{p^{2m(1-1/n)}} + \frac{\omega(p^{3m})}{p^{3m(1-1/n)}} + \dots \right) \right\}.$$

For $m \geq 2$ this converges unless $\deg(f) = n = 1$ or $m = n = 2$. An analogous definition can be made over any number field. Note that if $p \nmid \mathrm{disc}(f)$ then $\omega(p^k) = \omega(p)$ for each k, so that the pth term of the Euler product is $1 + \omega(p)(p^{m/n} - 1)/(p^m - p^{m/n})$.

Let $\omega'(r)$ be the number of pairs of residue classes (u,v) (mod r) with $\gcd(u,v,r) = 1$ for which $F(u,v) \equiv 0 \pmod{r}$. By the Chinese Remainder Theorem both $\omega(.)$ and $\omega'(.)$ are multiplicative functions. (Note that if $p \nmid f_0$ then $\omega'(p^k) = p^{k-1}(p-1)\omega(p^k)$.) We define V'_f to be the area of $\{(x,y) \in \mathbb{R}^2 : \ |F(x,y)| \leq 1\}$; and $A_f(\mathbb{Q})$ to be the number of distinct $\mathbb{Q}$-linear transformations $(x,z) \mapsto (\alpha x + \beta z, \gamma x + \delta z)$ of F for which $F(\alpha x + \beta z, \gamma x + \delta z) \equiv F(x,z) \mod (\mathbb{Q}^*)^2$. Comparing both sides of this equation, this happens if and only if $\rho \mapsto (\alpha\rho + \beta)/(\gamma\rho + \delta)$ is an automorphism of the roots ρ of $f(\rho) = 0$ (including $\rho = \infty$ if f has odd degree), and either $F(\alpha,\gamma)$ and $F(1,0)$ are non-zero with $F(\alpha,\gamma)/F(1,0) \in \mathbb{Q}^2$, or $\gamma = F(1,0) = 0$ with $\alpha\delta \in \mathbb{Q}^2$, or $F(\alpha,\gamma) = F(1,0) = 0$ and $\gamma \neq 0$ with $-(\alpha\delta - \beta\gamma) f'(\alpha/\gamma) \in \mathbb{Q}^2$. In the second case $\rho \mapsto (\alpha/\delta)\rho + \beta/\delta$, which implies that $\alpha/\delta = 1$ or -1; since $\alpha\delta \in \mathbb{Q}^2$ we deduce that $\alpha = \delta$ which implies that $\beta = 0$ and this transformation is thus the identity. Note that we must have $\alpha\delta - \beta\gamma \neq 0$. (In the appendix to [12] this is explored in detail and it is shown that $A_f(\mathbb{Q})$ must equal $1, 2, 3, 4, 6, 8$ or 12.) Let $N = m(g+1)$ and $\kappa'_f = \kappa'_{f,2}$ where

$$\kappa'_{f,m} := \frac{V'_f}{A_f(\mathbb{Q})} \prod_p \left\{ 1 + \left(1 - \frac{1}{p^{2m/N}}\right) \left(\frac{\omega'(p^m)}{p^{2m(1-1/N)}} + \frac{\omega'(p^{2m})}{p^{4m(1-1/N)}} + \dots \right) \right\}.$$

For $m \geq 2$ this converges unless $m = N = 2$, or $m = N = 3$, or $N = 4$ and $m = 2$. Analogous definitions and predictions can be made for any number field K. If $p \nmid f_0 \mathrm{disc}(f)$ then the pth term of the Euler product is $1 + \omega(p)(p-1)(p^{2m/N} - 1)/p(p^m - p^{2m/N})$.

One may think of V_f and V'_f as the local factors at infinity, to go with the local factors at the finite primes p in the products defining $\kappa_{f,m}$ and $\kappa'_{f,m}$.

2. Bounding the height of points on curves

A key tool in the proof of Theorem 1 is Theorem 5 from [12] which states:

Proposition 1. *Assume that the abc-conjecture is true. Suppose that $G(x,y) \in \mathbb{Z}[x,y]$ is homogenous, without any repeated factors. Then, for any coprime integers r and s,*

$$\prod_{\text{prime } p | G(r,s)} p \gg_G \max\{|r|,|s|\}^{\deg(G)-2-o(1)}.$$

Now, given a polynomial f without repeated roots, take $G(x,y) = y^{\deg(f)+1} f(x/y)$ and apply Proposition 1 to obtain the following result:

Corollary 2. *Assume that the abc-conjecture is true. Suppose that $f(x) \in \mathbb{Z}[x]$ is without repeated roots. Then, for any integer r,*

$$\prod_{\text{prime } p | f(r)} p \gg_f |r|^{\deg(f)-1-o(1)}.$$

Proof of Theorem 1 for integral points. We have integers d, t, r satisfying

$$d\,t^2 = f(r). \tag{1}$$

By Corollary 2 we have, assuming the *abc*-conjecture,

$$(|d||r|^{\deg(f)})^{1/2} \gg_f |d\,f(r)|^{1/2} = |d\,t| \geq \prod_{p|d\,t} p = \prod_{p|f(r)} p \gg_f |r|^{\deg(f)-1-o(1)},$$

and the result follows.

Proof of Theorem 1 for rational points. Homogenizing f to obtain F as above, we have

$$d\,t^2 = F(r,s) \tag{2}$$

for some integer t. Let $H = \max\{|r|,|s|\}$, so that $|F(r,s)| \ll_f H^{2g+2}$. Applying Proposition 1 we get, assuming the *abc*-conjecture,

$$|d|^{1/2} H^{g+1} \gg_f |d\,F(r,s)|^{1/2} = |d\,t| \geq \prod_{p|d\,t} p = \prod_{p|F(r,s)} p \gg_f H^{2g-o(1)},$$

and the result follows.

Theorem 1 is "best possible". Suppose that $f(x) = (x^2-1)g(x)$. For any fixed positive, non-square, integer D we know that there are arbitrarily large integer solutions (r,v) to $r^2 - 1 = D\,v^2$. Therefore if $d\,t^2 = f(r) = (r^2-1)g(r) = D\,v^2 g(r)$ with d squarefree then d divides $D\,g(r)$ and so $d \ll_g |r|^{\deg(g)} = |r|^{\deg(f)-2}$; that is $|r| \gg_f |d|^{1/(\deg(f)-2)}$. This same construction works whenever f has a factor of degree 2 over the rationals, call it $h(x)$ with leading coefficient $h_0 > 0$, and D is a positive integer such that Dh_0 is not a square, since one then knows that there are arbitrarily large integer solutions (r, v) to $h(r) = Dv^2$ whenever there is at least one, by the theory of the Pell equation.

Now assume that f has a factor $h(x)$ of degree 4 over the rationals, with $h(0) = 0$, so that $f(x) = h(x)g(x)$. Select any rational w for which $h(w) \neq 0$ and let D be the squarefree integer for which $D\,h(w) \in \mathbb{Q}^2$. It can be shown that for most w, the point (w, u) is a point of infinite order on the elliptic curve $D\,y^2 = h(x)$. Taking a large enough multiple of this point we obtain an arbitrarily large rational point $(r/s, v/s^2)$ on this curve, so that $d\,t^2 = F(r, s) = H(r, s)G(r, s) = D\,v^2 G(r, s)$. Hence d divides $D\,G(r, s)$ and so

$$|d| \ll_G \max\{|r|, |s|\}^{\deg(G)} = \max\{|r|, |s|\}^{2g-2}$$

and thus $|r|, |s| \gg_F |d|^{1/(2g-2)}$.

3. Heuristic in support of Conjecture 1

Suppose that $F(x, y) \in \mathbb{Z}[x, y]$ is homogenous of degree $2g + 2$, without any repeated factors. We wish to count the number of solutions to (2) in coprime integers r, s, with $D < d \leq 2D$. We saw, in the previous section, that the *abc*-conjecture implies that in any such solution to (2) we must have $|r|, |s| \ll D^{1/(2g-2)+o(1)}$.

For most pairs r, s with $X < \max\{|r|, |s|\} \leq 2X$, we have $F(r, s) \asymp X^{2g+2}$: the value can be significantly smaller, but only rarely, and then it can be no smaller than $X^{2g-o(1)}$ by Roth's Theorem. To simplify our heuristic we ignore this possibility (though this is taken into account in the proof of Theorem 2). Anyway, if $F(r, s) \asymp X^{2g+2}$, then we must have $t \asymp X^{g+1}/D^{1/2}$ in (2). Thus $X \gg X_0 := D^{1/(2g+2)}$.

For a fixed t the number of solutions to (2) with $X < \max\{|r|, |s|\} \leq 2X$ and $(r, s) = 1$ is around $(\omega'(t^2)/t^4)X^2$, and we expect a positive proportion of these values of d to be squarefree. Note that $\omega'(p^r) = p^{r-1}(p-1)\omega(p^r)$ if $p \nmid f_0$, and that $\omega(p^r) = \omega(p)$ if $p \not| \mathrm{disc}(f)$. Therefore, by a standard contour integration argument for summing coefficients of Dirichlet series, we know that $\omega'(t^2)/t^2$ is $\sim c_f(\log Y)^{\delta(f)-1}$ on average for values of t around Y, where $\delta(f)$ denotes the number of irreducible factors of f. Thus the total number of solutions to (2) with r, s in this range should be

$$\sum_{t \asymp X^{g+1}/D^{1/2}} \frac{\omega'(t^2)X^2}{t^4} \asymp_f X^2 \frac{(\log(X^{g+1}/D^{1/2}))^{\delta(f)-1}}{(X^{g+1}/D^{1/2})}$$

$$\asymp_f D^{1/2} \frac{(\log(X/X_0))^{\delta(f)-1}}{X^{g-1}},$$

where $X_0 = D^{1/(2g+2)}$. Now, summing over $X = X_0, 2X_0, \ldots 2^J X_0 = X_1$ with $X_1 = D^{1/(2g-2)+o(1)}$, we find that the expected number of solutions to (2) with $D < d \leq 2D$ when $g > 1$ is

$$\asymp D^{1/(g+1)}.$$

The main contribution to the above sum comes from those X with $X \ll X_0$, and when these are carefully summed up they give Conjecture 1(ii). Indeed we shall do this in the forthcoming proof of Theorem 2.

An analogous (but simpler) heuristic leads to Conjecture 1(i).

4. Theorems 2 and 4 for Integral Points

In this section we assume that the *abc*-conjecture is true; and that $f(x) \in \mathbb{Z}[x]$ has degree $n \geq 7$, and factors into distinct linear factors over $\mathbb{Q}$.

Proof of Conjecture 1(i) for f. We have seen that all solutions to (1) satisfy $|r| \ll |d|^{1/(n-2)+o(1)}$, assuming the *abc*-conjecture. Write $f(x) = c\prod_{i=1}^{n}(a_iX+b_i)$ where c, a_i, b_i are all integers with $(a_i, b_i) = 1$, so that $f_0 = ca_1 \dots a_n$. If $R < r \leq 2R$ with R sufficiently large then $\{|f_0| + o(1)\}R^n < |f(r)| < \{2^n|f_0| + o(1)\}R^n$. If (1) holds with $D < d \leq 2D$ then $\{|f_0|/2 + o(1)\}R^n/D < t^2 < \{2^n|f_0| + o(1)\}R^n/D$. Now, the number of $r \in (R, 2R]$ for which $f(r)$ is divisible by t^2 is $\omega(t^2)(R/t^2 + O(1))$. Therefore, for $R = (D\,T^2)^{1/n}$ and constants c_1 and c_2 satisfying $0 < c_1 < \sqrt{|f_0|/2}$ and $c_2 > \sqrt{2^n|f_0|}$, the number of such solutions to (1) is

$$\ll \sum_{c_1T<t<c_2T} \omega(t^2)(R/t^2+1) \ll (R/T+T)\log^n T$$

since $\omega(m) \ll n^{\#\{p:p|m\}}$. This gives $\ll D^{1/n}$ solutions in total for $T \ll D^{1/n}/\log^{n+\epsilon} D$, and in fact $o(D^{1/n})$ as $T \to \infty$. Unfortunately this just fails to cover the whole range $|r| \ll |d|^{1/(n-2)+o(1)}$, so this is where we use the fact that f is reducible.

Write each $a_ir + b_i = d_it_i^2$ with d_i squarefree so that $d_1 \dots d_n = dt_0^2$ and $t_0t_1 \dots t_n = t$, for some integer $t_0 \geq 1$ which is uniformly bounded in terms of the coefficients of f. We now show that there exists a divisor τ of t in the range $R^{1/3} < \tau \leq R^{2/3}$. If there exists t_i for which $t_i > R^{1/3}$ then let $\tau = t_i$; note that $t_i^2 \leq a_iR + b_i \leq R^{4/3}$ so that $t_i \leq R^{2/3}$. Otherwise let $\tau = t_1t_2 \dots t_j$ where j is chosen as small as possible so that this is $> R^{1/3}$; in this case $\tau = (t_1t_2 \dots t_{j-1})t_j \leq R^{1/3} {\cdot} R^{1/3} = R^{2/3}$. Also j exists since $(t_1 \dots t_n)^2 = t^2/t_0^2 \gg R^n/D \geq R^{2/3}$ if $T \gg D^{1/(3n-2)}$. Now $(t_i^2, t_j^2)|(a_ir + b_i, a_jr + b_j)|(a_ib_j - a_jb_i)$; hence, the fact that τ divides t implies that r is in one of $\omega(\tau_f^2)$ congruence classes $\pmod{\tau_f^2}$ for some integer τ_f, where τ/τ_f is an integer $\ll_f 1$. Therefore the number of such solutions to (1) is

$$\ll \sum_{R^{1/3}<\tau<R^{2/3}} \omega(\tau^2)(R/\tau^2+1) \ll R^{2/3}\log^n R,$$

which is $\ll D^{1/n}/(\log D)^{n/3}$, for $T \ll D^{1/4}/(\log D)^{n^2}$.

These two ranges for T allow us to account for all $|r| \ll |d|^{1/(n-2)+o(1)}$ provided $n \geq 7$. To obtain an asymptotic formula for the number of such values of d, we need only consider $|r| < D^{1/n}U$ as $U \to \infty$ slowly with D, by the above estimates. Theorem 2 in [8] implies that there are a bounded number of integer solutions (r, s) to $uf(r) = vf(s)$ where $u \neq v$ are given. Moreover there are a bounded number of integer solutions (r, s) to $f(r) = f(s)$

other than $s = r$ or $\ell - r$ (if such an ℓ exists). These results imply that the number of solutions to (1) with $d \le D$ is given by

$$\sum_{t \le T} \#\{r : |f(r)| \le D\,t^2,\ t^2 | f(r) \text{ and } f(r)/t^2 \text{ is squarefree}\}/A_f + o(D^{1/n})$$

as $T \to \infty$. Now the condition $|f(r)| \le D\,t^2$ is essentially equivalent to $|r| \le \{1 + o(1)\}(D\,t^2/|f_0|)^{1/n}$. If $t^2|f(r)$ then r is in one of $\omega(t^2)$ residue classes mod t^2. If that class is, say, r_0 then write $r = r_0 + t^2 s$ and then $g(s) = f(r_0 + t^2 s)/t^2$ and so we need to estimate $\#\{s : |s| \le S : g(s) \text{ is squarefree}\}$ where $S = S_t := \{1 + o(1)\}(D\,t^2/|f_0|)^{1/n}/t^2$. By the main result of [12] this is $\sim \prod_p (1 - \omega_g(p^2)/p^2) 2S$ (which can be shown to apply uniformly in this case) where $\omega_g(p^2)$ denotes the number of $m \pmod{p^2}$ for which $g(m) \equiv 0 \pmod{p^2}$. In fact if p^b is the exact power of p dividing t then $\omega_g(p^2) = \omega(p^{2b+2}, r_0)$ where $\omega(p^{2b+2}, r_0)$ is the number of $m \pmod{p^{2b+2}}$, with $m \equiv r_0 \pmod{p^{2b}}$ for which $f(m) \equiv 0 \pmod{p^{2b+2}}$. Thus if $t = \prod_i p_i^{b_i}$ then the contribution of the "t terms" to the sum above is

$$\begin{aligned} &\sim 2S_t \prod_{p \nmid t} \left(1 - \frac{\omega(p^2)}{p^2}\right) \prod_i \sum_{\substack{r_i \pmod{p^{2b_i}} \\ f(r_i) \equiv 0 \pmod{p^{2b_i}}}} \left(1 - \frac{\omega(p^{2b_i+2}, r_i)}{p^2}\right) \\ &= 2t^2 S_t \prod_{p \nmid t} \left(1 - \frac{\omega(p^2)}{p^2}\right) \prod_i \left(\frac{\omega(p^{2b_i})}{p^{2b_i}} - \frac{\omega(p^{2b_i+2})}{p^{2b_i+2}}\right); \end{aligned}$$

and then summing over t we obtain the first result.

Proof of Theorem 4(i). From the work of Bombieri and Pila [2] we know that there are $\ll R^{1/n}(\log R)^{O(1)}$ pairs of distinct integers $r_1, r_2 \in [R, 2R]$ for which $t_2^2 f(r_1) = t_1^2 f(r_2)$, uniformly for any given t_1, t_2. Thus the number of d for which C_d has a pair of non-trivial integer points $f(r_1) = d\,t_1^2, f(r_2) = d\,t_2^2$ with $t_1, t_2 \le T = R^{(1/3)(1/n - 1/n^2)}$ is $\ll T^2 R^{1/n}(\log R)^{O(1)}$, which is certainly acceptable. For larger d we simply bound the number of twists with two points by the number with one point, for want of a better argument, and we obtain our result.

5. Proof of Theorem 2 for Rational Points

Define F from f as above. Define $S(R, z)$ to be the set of pairs of coprime integers (r, s) such that $R < \max\{|r|, |s|\} \le 2R$ for which $0 < |F(r, s)| \le R^n/z$. By Roth's theorem $S(R, z)$ is empty if $z \gg R^{2+o(1)}$.

We claim that if $1 \le z \le R$ then $|S(R, z)| \asymp_f R^2/z$: For $z \ll 1$ this is trivial. Otherwise, write $F(x, y) = c \prod_{i=1}^n (a_i X + b_i Y)$ where c, a_i, b_i are all integers with $(a_i, b_i) = 1$, so that $f_0 = c a_1 \ldots a_n$. Since $\max\{|a_i r + b_i s|, |a_j r + b_j s|\} \asymp R$, we see that there exists i such that $|a_i r + b_i s| \ll R/z$ while $|a_j r + b_j s| \asymp R$ for all $j \ne i$. Now if $a_i \ne 0$ then $-R/(z a_i) - b_i s/a_i \ll r \ll R/(z a_i) - b_i s/a_i$ so that there are $\asymp R/(z a_i)$ possibilities for r, for each s, and thus we obtain the claim.

Now define $N(R,z)$ to be the number of $(r,s)\in S(R,z)$ such that $F(r,s)=D\,t^2$ where d is squarefree and $D\le d\le 2D$. The *abc*-conjecture tells us that in any such solution $\max\{|r|,|s|\}\le D^{1/(n-4)+o(1)}$.

Now, $N(R,z)\le |S(R,z)|\asymp_f R^2/z$, so that $\sum_{j\ge 0} N(D^{1/n}\cdot 2^j, 2^{(2+\epsilon)j})\ll D^{2/n}$.

Given residue classes $1\le u,v<m$ which are coprime with m, and integers a,b, we will need an uniform estimate for the number of pairs of integers r,s satisfying $|ar+bs|\le X$ and $vr\equiv us \pmod m$. In fact the pairs (r,s) lie on the lattice generated by $(u,v),(m,0)$ and $(0,m)$ which has determinant m. The number of lattice points in this region can be estimated by $1/m$ times its volume, with an error no bigger than some multiple of the length of its perimeter.

If $R=(DT^2)^{1/n}$ where $z\le T^2$ then $t\asymp T/\sqrt{z}$. Thus we have $t^2|F(r,s)$ where $|a_ir+b_is|\ll R/z$ and $|r|,|s|\ll R$ and so, by the above, the number of lattice points is $\ll \omega(t^2)(R^2/zt^2+R)$. Summing over all t, the number of lattice points is

$$\ll (R^2/(\sqrt{z}T)+RT/\sqrt{z})\log^n(T/\sqrt{z}).$$

This is $o(D^{2/n})$ whenever $T\le D^{1/(n+2)}/(\log D)^{n-2}$ provided $T\to\infty$; and for $z\ge (T^{n+2}/D)^{2/n}\log^{2n+1}T$ for larger T (provided $n\ge 5$).

We use the fact that f is reducible. Write each $a_ir+b_is=d_it_i^2$ with d_i squarefree so that $d_1\dots d_n=d$ and $t_1\dots t_n=t$. We now show that there exists a divisor τ of t in the range $(R/z)^{1/3}<\tau\ll\max\{(R/z)^{2/3},R^{1/2}\}$. If there exists t_i for which $t_i>(R/z)^{1/3}$ then let $\tau=t_i$; note that $t_i^2\le(|a_i|+|b_i|)R\ll R$. Otherwise let $\tau=t_1t_2\dots t_j$ where j is chosen as small as possible so that this is $>(R/z)^{1/3}$; in this case $\tau=(t_1t_2\dots t_{j-1})t_j\le (R/z)^{1/3}\cdot (R/z)^{1/3}$. Also j exists since $(t_1\dots t_n)^2=t^2\gg R^n/Dz\ge (R/z)^{2/3}$ if $z\ll (T^{3n-2}/D)^{2/n}$. Therefore, since $(t_i^2,t_j^2)\mid(a_ir+b_is,a_jr+b_js)\mid(a_ib_j-a_jb_i)(r,s)=a_ib_j-a_jb_i$, the fact that τ divides t implies that r/s is in one of $\omega(\tau_f^2)$ congruence classes $\pmod{\tau_f^2}$ for some integer τ_f, where τ/τ_f is an integer $\ll_f 1$. Therefore the number of such solutions to (2) is

$$\ll \sum_{(R/z)^{1/3}<\tau\ll R^{2/3}} \omega'(\tau^2)(R^2/z\tau^2+R)\ll R^{5/3}\log^n R,$$

which is $\ll D^{2/n}/\log^2 D$ since $R\le D^{1/(n-4)+o(1)}$.

Combining the above gives the result that the number of such d is $\ll D^{2/n}$ as $n\ge 25$, and one finds that there is a significant contribution to the main term only when $z,T\ll 1$.

To obtain the constant κ_f' we proceed much as in Theorem 2. The modular arithmetic proceeds much as before. The contribution of the size of the numbers in the definition of κ_f was $2|f_0|^{-1/n}$, which is obtained from $\lim_{U\to\infty}|\{x\in\mathbb{R}:|f(x)|\le U\}/U^{1/n}$. Here the analogous contribution is $\lim_{U\to\infty}|\{x,y\in\mathbb{R}:|F(x,y)|\le U\}/U^{2/n}=V_f$, and thus the result.

Remark. The argument used to bound the number of C_d with two integral points (i.e. the proof of Theorem 4(i)) does not seem to go through here: although Heath-Brown showed that there are $\ll R^{2/n}(\log R)^{O(1)}$ rational points on $f(r_1/s_1)t_2^2=f(r_2/s_2)t_1^2$ with $r_1,s_1,r_2,s_2\le R$ for any given t_1,t_2, we actually need to bound points on $F(r_1,s_1)t_2^2=F(r_2,s_2)t_1^2$.

6. *abc*-THEOREMS FOR POLYNOMIALS.

In this section we establish unconditional results that are analogous to Proposition 1 and Corollary 2 for polynomials, which do not seem to have been observed previously:

Proposition 2. *a) Suppose that $g(x) \in \mathbb{C}[x]$ has no repeated roots. For any $r(t) \in \mathbb{C}[t]$ we have*

$$\#\{\alpha \in \mathbb{C} : \ g(r(\alpha)) = 0\} \geq \deg(r)(\deg(g) - 1) + 1.$$

b) Suppose that $G(x, y) \in \mathbb{C}[x, y]$ is homogenous, without any repeated factors. For any coprime polynomials $r(t), s(t) \in \mathbb{C}[t]$, we have

$$\#\{\alpha \in \mathbb{C} : \ G(r(\alpha), s(\alpha)) = 0\} \geq \max\{\deg(r), \deg(s)\}(\deg(G) - 2) + 2.$$

Proof. a) follows from the fact that any polynomial r has exactly $\deg(r) - 1$ critical points counted with multiplicity, and b) from the fact that any rational function r/s on $\mathbb{P}^1$ has exactly $2\deg(r/s) - 2$ critical points counted with multiplicity. The proof also implies that the results here are best possible.

7. Pairs of Points on the same twists

Suppose that we have two solutions to (1) for a given d; that is $d\,u^2 = f(x)$ and $d\,v^2 = f(y)$. This then gives a solution to

$$z^2 = f(x)f(y) \tag{3}$$

with $z = \pm duv$. Thus, for a given f, the set of pairs of different solutions to (1) with $u, v > 0$, as we vary over d, is in 1-1 correspondence with the set of solutions to (3) with $z > 0$, once we have discarded the "trivial" solutions with $z = 0$, and the "repeat solutions" with $x = y$.

A surface of general type: Proof of Theorem 3

In order to apply the Bombieri-Lang conjecture we need to know that the surface defined by (3) is of general type. Ernst Kani provided me with the following proof. Let $n = 2g+2 \geq 6$ (so that $g \geq 2$). Applying a Möbius transformation if necessary, we may assume that f has degree n. Let $X = \{(x, y, z) : z^2 = f(x)f(y)\}$ and view X as a double cover of $\mathbb{P}^1 \times \mathbb{P}^1$. Then $H := A_1 \times \mathbb{P}^1 + \mathbb{P}^1 \times A_2$ (for points A_1, A_2) is an ample divisor on $Y = \mathbb{P}^1 \times \mathbb{P}^1$, and the canonical divisor on Y is $K_Y = -2H$. Moreover, the divisor D defined by $f(x)f(y) = 0$ is linearly equivalent to nH ($D \sim nH$) and has only simple singularities. Thus, if $p : X$ denotes the de-singularized double cover (as in [1], p. 182), then by equation (8) there we have

$$K_X \sim p^*(-2H + (n/2)H) = p^*(mH), \text{ with } m = (n - 4)/2.$$

Thus, for any $k > 0$,

$$h^0(kK_X) = h^0(p^*(kmH)) \geq h^0(kmH) \sim ck^2m^2 \tag{4}$$

for some constant $c \neq 0$, the latter because H is ample. Here $h^0(D) = \dim H^0(X, L(D))$, for any divisor D on X (and similarly for divisors on Y). But (4) implies that X has Kodaira dimension 2 (i.e. X is of general type) when $m > 0$ (i.e. $n > 4$).

Since X is of general type we can apply the Bombieri-Lang conjecture, and so we wish to understand the proper closed subvariety $S \subset X$. Since S is a proper closed subvariety we may assume that S is a finite union of curves, and since we may discard finitely many points, we may assume that all of those curves have genus 0 or 1 (by Faltings' Theorem).

Counting pairs of points: Proof of Theorem 4(ii)

We have just seen that the $d \leq D$ for which $c_d(\mathbb{Q}) \geq 2$ arise, other than in finitely many examples, from points on finitely many curves of genus 0 and 1 on the surface (3). The number of such $d \leq D$ arising from curves of genus 1 is $D^{o(1)}$, a relatively small quantity, so we can now restrict our attention to those d that arise from curves of genus 0. These curves may always be parameterized by rational functions, that is we can find $x(t), y(t) \in \mathbb{C}(t)$ for which $f(x(t))f(y(t)) \in \mathbb{C}(t)^2$.

Recall that f has degree $2g+2$ with $g \geq 2$, and $F(X,Y) = f(X/Y)Y^{2g+2}$. We will write $x(t) = r(t)/s(t)$ and $f(r(t)/s(t)) = d(t)(u(t)/s(t)^{g+1})^2$ with $d(t), r(t), s(t), u(t) \in \mathbb{C}[t]$, where $d(t)$ has no repeated roots, and $s(t)$ has no roots in common with $r(t)u(t)$; and similarly $y = R(t)/S(t)$. Let $\delta = \max\{\deg(r), \deg(s)\}$ be the degree of $x(t)$, which we may assume to be $\leq \delta'$, the degree of $y(t)$. We may find a Mobius transformation $t \mapsto Mt$ to ensure that $F(r(t), s(t))$ has degree $2\delta(g+1)$ and that $F(R(t), S(t))$ have degree $2\delta'(g+1)$ (i.e. there is no cancellation in either product).

By Proposition 2b we have $\deg(u) \leq 2\delta - 2$, and so $d(t)$ has degree $\geq 2\delta(g-1) + 4$. Therefore $\deg d(t) \in [2\delta(g-1)+4, 2\delta(g+1)]$, so we deduce that

$$2\delta'(g-1) + 4 \leq 2\delta(g+1).$$

Thus if $\delta \leq g/2$ then $\delta' = \delta$ (else $\delta' \geq \delta + 1$ whence $(\delta+1)(g-1) + 2 \leq \delta(g+1)$ giving a contradiction). Note that if $\delta = 1 (\leq g/2)$ then $\delta' = 1$ and so $\deg u = \deg U = 0$; therefore the two solutions are connected by an automorphism, so are of no interest to us. We henceforth assume $\delta \geq 2$.

Now $d(t)$ has even degree $\geq 2\delta(g-1) + 4 \geq 4g$ for $\delta \geq 2$. The number of such integers $d \leq D$ is $\ll D^{1/2g}$ assuming Conjecture 1(ii); and $\ll D^{1/(2g-2)+o(1)}$ assuming the *abc*-conjecture by Corollary 2(ii).

Remark. These bounds improve to $\ll D^{1/(2g+1)}$ and $\ll D^{1/(2g-1)+o(1)}$, respectively, when $d(t)$ has degree $> 4g$. If $d(t)$ has degree $4g$ then $\deg U = \frac{1}{2}(2\delta'(g+1) - \deg d) = \delta'(g+1) - 2g$, whereas $\deg U \leq 2\delta' - 2$ by Proposition 2b and therefore $\delta' \leq 2$. Thus $\delta = \delta' = 2$, and so there exist rational functions $x(t)$ and $y(t)$ of degree 2, not in the same orbit of $\mathrm{Aut}(C)$, for which $f(x(t))/f(y(t))$ is the square of a rational function of degree 2. It may be that there does not exist such an exotic example when f has large enough degree.

Numerous twists with pairs of points:

- Let $f(x) = xh(x(2-x))$ for a given $h(x) \in \mathbb{Z}[x]$ of degree $g \geq 1$, so that $n = 2g+1$. We get a rational solution $x = u, y = 2-u$ to (3) if and only if $u(2-u) \in \mathbb{Q}^2$. This occurs if and only if $u = (t+1)^2/(t^2+1)$ for some rational t, in which case $u(2-u) = ((t^2-1)/(t^2+1))^2$. Thus u and $2-u$ are the x-coordinates of rational points on C_d where

$$d = (t^2+1)^{2g+1}h(((t^2-1)/(t^2+1))^2).$$

By Conjecture 1(ii) the number of such $d \leq D$ is $\sim \kappa'_f D^{1/(2g+1)}$.

- Let $f(x) = (x-1)(x-2)(x-4)...(x-2^{n-1})$. We get a rational solution $x = u, y = 2u$ to (3) if and only if $2^{n-1}(2u-1)(u-2^{n-1}) \in \mathbb{Q}^2$. This occurs if and only if $u = 2^{n-1}(t^2-1)/(t^2-2^n)$ for some rational t. In this case with n divisible by 4, u and $2u$ are the x-coordinates of rational points on C_d where

$$d = (2^n-1)\prod_{j=1}^{n-1}((2^j-1)t^2 + (2^n-2^j)).$$

By Conjecture 1(ii) the number of such $d \leq D$ is $\sim \kappa'_f D^{1/(2g+1)}$.

- Let $f(x) = x^4 - 4ax^2 - a^2$. We get a rational solution $x = t + a/t,\ y = at/(t^2-a)$ to (3) in rational functions of degree 2 that are not in the same orbit of $\mathrm{Aut}(C)$, where $f(x(t))/f(y(t)) = (i(t^2-a)^2/at^2)^2$ is the square of a rational function of degree 2.

Several interesting future projects emerge from these considerations:

- Classify all $f(x) \in \mathbb{C}[x]$ and $x(t), y(t) \in \mathbb{C}(t)$ of degree two for which $f(x(t))/f(y(t))$ is the square of a rational function of degree 2. I guess that if $\deg(f)$ is sufficiently large then $x(t)$ and $y(t)$ must be in the same orbit of $\mathrm{Aut}(C)$.
- Classify all $f(x) \in \mathbb{C}[x]$ and $x(t), y(t) \in \mathbb{C}[t]$ which give rise to solutions to (3). In other words we wish to understand pairs of integral points on the C_d. Florian Luca and I have shown that there are no solutions with $\deg(f) > 2 = \deg(x) = \deg(y)$. I guess that if $\deg(f)$ is sufficiently large then $x(t)$ and $y(t)$ must be in the same orbit of $\mathrm{Aut}(C)$; this implies Conjecture 2(i) assuming the Bombieri-Lang conjecture.
- Classify all $f(x) \in \mathbb{C}[x]$ and $x(t), y(t), Y(t) \in \mathbb{C}(t)$ which give rise to two solutions to (3). That is, to determine triples of rational points on C_d; were the triples to give rise to solutions of (3) involving distinct polynomials then there would be finitely many triples, by Faltings' theorem, unless the polynomials had extremely low degree. In any case we believe that if $\deg(f)$ is sufficiently large then two of any triple of solutions lie in the same orbit of $\mathrm{Aut}(C)$; this should lead to a proof of Conjecture 2(ii) assuming the Bombieri-Lang conjecture.

8. Only finitely many twists with pairs of points

Theorem 5(i). *Assume the abc-conjecture. Let $f(x) \in \mathbb{Z}[x]$ have degree n and no repeated roots. If there exists a polynomial $h(x) \in \mathbb{Z}[x]$ of degree $\ell < n$ with no roots in common* *with $f(x)$, such that $g(x) := f(x) - h(x)$ has μ distinct roots and*

$$n > \frac{5+\sqrt{17}}{10}\ (4\ell + 5\mu)$$

then there are only finitely many squarefree integers d for which there is more than one non-trivial integer solution to $f(x) = d\,y^2$.

Proof. Let m be the number of distinct roots of gh so that $\mu \le m \le \mu + \ell$. Suppose that $f(r) = d\,u^2$ and $f(s) = d\,v^2$ for integers d, r, s, u, v with d squarefree and $|r| \le |s|$. Now $g(r)+h(r) = d\,u^2$, so applying the *abc*-conjecture we deduce that $|r|^{n-o(1)} \asymp |g(r)|^{1-o(1)} \ll \prod_{p|d\,u(gh)(r)} p \ll |d\,u||r|^m$; and therefore $|u| \ll |d|u^2|r|^{m-n+o(1)} \ll |r|^{m+o(1)}$. Similarly $|v| \ll |s|^{m+o(1)}$. Define α, β so that $|u| = |r|^{\alpha m}$ and $|v| = |s|^{\beta m}$, and thus $0 \le \alpha, \beta \le 1 + o(1)$.

Since $|r| \le |s|$ thus $u^2|h(s)| \ll v^2|h(r)|$. Let $\gamma = \gcd(v^2 g(r), u^2 g(s))$ and so $v^2 g(r)/\gamma + (v^2 h(r) - u^2 h(s))/\gamma = u^2 g(s)/\gamma$. By the *abc*-conjecture we find that $|v^2 g(r)/\gamma|^{1-o(1)} \ll (v^2|h(r)|/\gamma)|uv||rs|^{\mu}$; and so $|r|^{n-\ell-\mu-m\alpha-o(1)} \ll |s|^{\mu+\beta m}$.

Noting that $|r|^{n-2m\alpha} = |r|^n/u^2 \asymp f(r)/u^2 = d = f(s)/v^2 \asymp |s|^n/v^2 = |s|^{n-2m\beta}$, we deduce that

$$(n - \ell - \mu - m\alpha)(n - 2m\beta) \le (\mu + \beta m)(n - 2m\alpha) + o(1).$$

Since the difference of the two sides of this equation is linear in α and β separately, the extreme cases of the inequality must happen at the endpoints for the ranges of α and β (that is at 0 or $1 + o(1)$). We then easily prove that $|r|, |s| \ll 1$ for

$$n > \max\left\{ 2m + \ell + 2\mu, \frac{\ell + 2\mu + 3m + \sqrt{\ell^2 + 4\mu^2 + 9m^2 + 4\ell\mu - 2\ell m + 4m\mu}}{2} \right\}.$$

(The extreme cases here correspond to $\beta = 1+o(1)$ and to $\alpha = 1+o(1)$ and 0, respectively). This lower bound for n is an increasing function of m in its range $\mu \le m \le \mu + \ell$, so the theorem holds since the bound given is larger than the above expression taken with $m = \mu + \ell$.

Examples. The hypothesis, and hence the result, of Theorem 5(i) holds for $f(x) = g(x) + a$ where a is a non-zero constant provided $n > (5 + \sqrt{17})m/2$, where m is the number of distinct roots of $g(x)$. In particular for $f(x) = x^n + a$ once $n \ge 5$. The hypothesis also holds for $f(x) = x^n + ax + b$ once $n \ge 9$; and indeed for any $f(x) = x^n + h(x)$ with $h(0) \ne 0$, provided the degree of h is $\le (n - 5)/4$

We want to use an analogous argument to find $f(x)$ for which there are only finitely many squarefree d with more than one non-trivial rational point on $f(x) = d\,y^2$. However there is now no guarantee that $h(r)$ and $h(s)$ are small, so we need to rework the third application of the *abc*-conjecture in the proof above. To do so we will use the following generalization of the *abc*-conjecture:

The ***abcd*****-conjecture.** *If a, b, c and d are integers for which $a+b+c+d=0$, where no subsum vanishes and $\gcd(a,b,c,d)=1$, then*

$$|a|, |b|, |c|, |d| \ll \ N(abcd)^{3+o(1)}.$$

The exponent 3 is conservative based on the example $2^{3k} + 3 \times 2^k \times (2^k+1) + 1 - (2^k+1)^3 = 0$. A less conservative version of the conjecture is that the exponent should be 1 outside of "finitely many subvarieties" (the above example belongs to the subvariety $\{a+b+c+d=0, b^3 = 27acd\}$).

Theorem 5(ii). *Assume the abc-conjecture and abcd-conjecture. Let $f(x) \in \mathbb{Z}[x]$ have degree n and no repeated roots. If there exists a polynomial $h(x) \in \mathbb{Z}[x]$ with no roots in common with $f(x)$, such that $h(x)(f(x)-h(x))$ has $< n/10$ distinct roots, then there are only finitely many squarefree integers d for which there is more than one non-trivial rational solution to $f(x) = d\,y^2$.*

Sketch of Proof. We have $|u| \ll |r|^{m+o(1)}$ and $|v| \ll |s|^{m+o(1)}$ as in the proof of Theorem 5(i). Again define α, β so that $|u| = |r|^{\alpha m}$ and $|v| = |s|^{\beta m}$, and thus $0 \le \alpha, \beta \le 1 + o(1)$.

Now we will let $\gamma = \gcd(v,u)$ and consider the equation

$$g(r)(v/\gamma)^2 + h(r)(v/\gamma)^2 = g(s)(u/\gamma)^2 + h(s)(u/\gamma)^2.$$

By the *abcd*-conjecture we find that $|g(r)(v/\gamma)^2|^{1/3-o(1)} \ll |uv/\gamma^2||rs|^m$; which can be rewritten as $|r|^{n/3-m-\alpha m-o(1)} \ll |s|^{m+\beta m/3}$, so that

$$(n-2m\beta)(n/3-m-\alpha m) \le (n-2m\alpha)(m+\beta m/3) + o(1).$$

This cannot hold if $n > 10m$.

Remark. If we can take exponent A instead of 3 in the *abcd*-conjecture, we get a contradiction if $n > (3A+1)m$.

9. Discussion

Different models of a curve, and integral points

The choice of model for a hyperelliptic curve has little effect on the number of rational points. However integral points are not so robust a notion since their definition does depend on the chosen model for the curve. For example, rational points (r,s) on $dy^2 = x^3+1$ are in 1-to-1 correspondence with rational points (u,v) on $dy^2 = x^4 + x$ (via the birational transformation $u = 1/r, v = s/r^2$), yet Conjecture 1 predicts quite different quantities of integral points on the quadratic twists of these two models for the same curve.

Are our predictions made on a firm basis?

Many researchers are skeptical about the full Bombieri-Lang conjecture, not least because of the extraordinary deductions that can be made from it, such as the results from [4] mentioned in the introduction. One further consequence of the work of [4] is that if we fix $g > 1$ and any number field K with $[K:\mathbb{Q}] \gg_g 1$ then there are only finitely many curves C of genus g defined over $\mathbb{Q}$ such that there is a point in $C(K)$ which does not belong to a subfield of K (else the point has $[K:\mathbb{Q}]$ *distinct* conjugates in $C(L)$ where L is the Galois closure of $K/\mathbb{Q}$, contradicting the universal bound on the number of rational points given by [4]). At first glance this seems implausible, but perhaps the conjecture is true and rational points are very rare indeed, requiring many of us to gain new intuitions.

10. When there are infinitely many points

If $g = 0$ or 1, our argument with the *abc*-conjecture does not give an upper bound on the height of solutions, which is just as well, since one knows that there can be solutions of arbitrarily large height. Nonetheless we can exploit several other ideas in this article to guess at the distribution of small points.

Extending our heuristics to curves of genus 0

We shall assume here that f has degree 2. By the heuristic of section 3, we expect $\asymp_f XD^{1/2}(\log(X/D^{1/2}))^{\delta(f)-1}$ rational points on C_d with $d \asymp D$ and $\max\{|r|,|s|\} \asymp X$, where $X \gg D^{1/2}$: in particular, $\asymp_f D$ rational points when $X \asymp D^{1/2}$. This is all more-or-less confirmed by known results on conics. Legendre's theorem states that there are solutions to (2) if and only if d and its prime factors belong to certain residue classes mod ℓ where $\ell = \ell(f)$ is a certain nonzero integer depending on f (for example, if $f = ax^2+b$ then $\ell = 4ab$). Considering only prime values of d we see that there are indeed $\asymp D(\log D)^{O(1)}$ integers $d \in (D, 2D]$ for which (2) has solutions. Moreover, Holzer's well-known bound [13] on the height of points on a conic (if there is a non-zero integer solution to $ax^2+by^2 = cz^2$ where abc is squarefree then there is one with $|ax^2|, |by^2|, |cz^2| \le |abc|$) translates to the fact that if there is a non-trivial solution to (2) then there is one with $|r|, |s| \ll |d|^{1/2}$; thus we do indeed have the predicted number and size of solutions.

We can extend the heuristic in section 3 to the easier case of solutions to (1), i.e. integral points, when f has degree two, predicting $\asymp_f D^{1/2}(\log(X/D^{1/2}))^{\delta(f)-1}$ integral points on C_d with $d \asymp D$ and $|r| \asymp X$, whenever $X \gg D^{1/2}$. The key question is in what range for X is this true uniformly? In the range in which we can prove it holds, that is X not much bigger than $D^{1/2}$, the factor $(\log(X/D^{1/2}))^{\delta(f)-1}$ has little effect no matter what the value of $\delta(f)$, and my guess is that this remains so. Therefore let us predict $\asymp_f D^{1/2+o(1)}$ integral points uniformly in each dyadic interval $[X, 2X]$, for X up to $\exp(D^{1/2+o(1)})$: the reason I choose this limit is that there are $D^{1/2+o(1)}$ dyadic intervals up to this height, and therefore a total of about $D^{1+o(1)}$ such points. This fits well with the theory of the Pell equation since we know that if $f(x) = x^2 - 1$ then (1) has solutions for a positive proportion of squarefree d. Moreover Dirichlet's class number formula (or, indeed, the construction of fundamental units using continued fractions) implies that the smallest such solutions always have $|r| \le \exp(d^{1/2+o(1)})$. In fact our heuristic suggests that most such fundamental solutions are this large, and hence that the class numbers of the corresponding real quadratic fields are typically very small, supporting well-known predictions of Cohen and Lenstra [5,6].

Extending our heuristics to rational points on curves of genus 1

It is widely believed that, asymptotically, half of the quadratic twists of any given elliptic curve over the rationals have finitely many rational points, and half have rank one (see [3] for a survey).

The method of Gouvêa and Mazur [11], as refined by Stewart and Top [16] and Rubin and Silverberg [15], constructs roughly the predicted number of curves with non-trivial solutions to (2) when $g > 1$. Their technique only finds rational points of small size (polynomial in d), which is all that there is for $g > 1$ assuming the *abc*-conjecture, by Theorem 1. However, for $g = 1$, the heuristic of section 3 predicts that there are just $D^{1/2+o(1)}$ twists with such small non-trivial rational points and indeed their method counts this many, far fewer than "half the quadratic twists" (as in the previous paragraph). If we assume that the range of validity of the prediction of section 3 can be extended for all X up to $\exp(D^{1/2+o(1)})$ (as we did for integral points on curves of genus 0 in the previous section) then we get a total of $D^{1+o(1)}$ such rational points, and so we might be led to predict that all of the generators of the Mordell-Weil group of C_d are $\ll \exp(d^{1/2+o(1)})$. Such a prediction can be deduced assuming the weak Birch-Swinnerton Dyer conjecture and the Riemann Hypothesis for $L(C_d, s)$, as in [14].

One recently popular question is to estimate, for a given elliptic curve E, the number of squarefree $d \leq D$ for which the dth quadratic twist of E has rank $r \geq 2$. Based on the growth of the coefficients of certain modular forms, Sarnak predicted something like $D^{3/4+o(1)}$ such twists with rank ≥ 2, whereas, based on computational evidence, Rodriguez-Villegas predicted something like $D^{3/4}(\log D)^{O(1)}$ such twists with rank 2. Conrey, Keating, Rubinstein and Snaith [7] developed a sharper prediction, $\sim c_E D^{3/4}(\log D)^{3/8+\eta_E}$ such twists of rank 2, based on (the GUE) conjectures for the distribution of values of L-functions, where η_E depends explicitly on $E[2]$ and $\mathrm{Disc}(E)$ (see [9]). Now [14] also predicts, again assuming the Birch-Swinnerton Dyer conjecture and the Riemann Hypothesis for $L(C_d, s)$, that the smallest generator of the Mordell-Weil group of C_d is $\ll \exp(d^{1/2r+o(1)})$, when it has rank r. Combining this with our extenstion of the heuristic of section 3, we predict that there are $\ll D^{1/2+1/2r+o(1)}$ squarefree $d \leq D$ for which the dth quadratic twist of E has rank r. When $r = 2$ this coincides with the predictions of Sarnak, Rodriguez-Villegas, and Conrey et al.

There has been speculation that the number of quadratic twists of rank 3 should grow like $D^{3/4+o(1)}$, that is, roughly as many as of rank 2 (see Remark 8.3 of [15]), whereas our prediction gives $\ll D^{2/3+o(1)}$, far fewer. Rubin and Silverberg [15] constructed $\gg D^{1/2}$ quadratic twists of rank ≥ 2, $\gg D^{1/3}$ quadratic twists of rank ≥ 3 and $\gg D^{1/6}$ quadratic twists of rank ≥ 4, assuming only the parity conjecture, by creating elliptic curves with several rational points of small height; however these points are smaller than what we would predict is typical, so we believe that their lower bounds fall well short of the actual count.

In a further article, with Mark Watkins, we will develop this heuristic approach to give new evidence in favor of Honda's conjecture that there is an absolute bound on the rank of the elliptic curves in the family of quadratic twists of a given elliptic curve.

11. Superelliptic curves.

The methods, results and conjectures of our study of hyperelliptic curves carry over to the quadratic twists $C_d:\ d\,y^m = f(x)$ of a given *superelliptic curve*, $C = C_1$ where $m \geq 3$, $f(x)$ is a polynomial with integer coefficients, whose factors have multiplicity less than m, and d is not divisible by the mth power of any prime. For simplicity we will make the further assumptions that f has no repeated roots (which is so in most cases of interest), and usually that the degree of f is divisible by m (which simplifies matters considerably when we consider rational points). We again define $c_d(\mathbb{Z})$ and $c_d(\mathbb{Q})$ to be the number of automorphism classes of non-trivial integral and rational points on C_d, respectively.

Throughout the rest of this section we assume the *abc*-conjecture.

We conjecture that there are $\sim \kappa_{f,m} D^{1/\deg(f)}$ mth-power free integers d with $|d| \leq D$ for which $c_d(\mathbb{Z}) \neq 0$, provided $\deg(f) \geq 2$, and that there are $\sim \kappa'_{f,m} D^{2/\deg(f)}$ mth-power free integers d with $|d| \leq D$ for which $c_d(\mathbb{Q}) \neq 0$, except perhaps when $\deg(f) \leq m = 3$. The results in [12] can again be used to deduce that the implicit lower bounds hold; and we can even prove these conjectures if $f(x)$ factors into distinct linear factors over $\mathbb{Q}$ and has degree $> 4m(m+1)/(m-1)^2$.

We also conjecture that if $\deg(f)$ is sufficiently large then there are only finitely many mth-power free integers d for which $c_d(\mathbb{Z}) > 1$, and only finitely many mth-power free integers d for which $c_d(\mathbb{Q}) > 2$. Again we can exhibit certain infinite families of curves, C, for which these conjectures are true, assuming the *abc*-conjecture.

Any integral point on C_d with x-coordinate r satisfies $|r| \ll |d|^{1/(\deg(f)-\frac{m}{m-1})+o(1)}$. For f of degree $mg+i,\ 1 \leq i \leq m$, any rational point on C_d with x-coordinate r/s where $(r,s) = 1$ satisfies

$$|r|, |s| \ll |d|^{1/\left(mg+i-1-\frac{(m,i)+1}{m-1}\right)+o(1)}. \tag{5}$$

Thus we can deduce that there are $\ll_f D^{1/(\deg(f)-\frac{m}{m-1})+o(1)}$ mth-power free integers d with $|d| \leq D$ for which $c_d(\mathbb{Z}) \neq 0$ (which is non-trivial unless $\deg f \leq 2$); and that there are $\ll_f D^{2/\left(mg+i-1-\frac{(m,i)+1}{m-1}\right)+o(1)}$ mth-power free integers d with $|d| \leq D$ for which $c_d(\mathbb{Q}) \neq 0$ (which is non-trivial unless $\deg f \leq 3$, or $\deg f = 4$ and $m = 3$ or 4). It may be that these results can be improved. To prove (5) let $F^*(r,s) = s^{mg+i} f(r/s)$ so that $F(r,s) = F^*(r,s) s^{m-i}$. Any rational point on C_d gives rise to a solution of $F(r,s) = d\,t^m$, so we may write $F^*(r,s) = d_1 t_1^m,\ s^{m-i} = d_2 t_2^m$, where $d_1 d_2 = d\,t_0^m$ and $t = t_0 t_1 t_2$ with $t_0 \ll 1$. The key here is the bound $\prod_{p|s} p^m \leq d_2^{m-1} |s|^{(m,i)}$ which is easily proved by considering the cases where $p | d_2$ and $p \nmid d_2$ separately. Therefore, by the *abc*-conjecture, we have

$$H^{mg+i-1-o(1)} \ll \prod_{p|sF^*(r,s)} p = \prod_{p|dt} p \leq \prod_{p|d_1t_1} p \prod_{p|s} p \leq |d_1 t_1| \prod_{p|s} p,$$

and so $H^{m(mg+i-1)-o(1)} \ll d^{m-1} |F^*(r,s)| |s|^{(m,i)} \ll d^{m-1} H^{mg+i+(m,i)}$ and the result follows.

Assuming the Bombieri-Lang conjecture for surfaces of the form $z^m = g(x)/g(y)$ where $g(X) \in \mathbb{Z}[X]$ has degree divisible by m, the set of mth-power free integers d for which

$c_d(\mathbb{Q}) \geq 2$ may be parameterized by the rational points on a finite number of curves of genus 0 and 1, together with finitely many exceptional d; in fact there are $\ll D^{4/m(n-1)}$ such integers $d \leq D$ for which $c_d(\mathbb{Q}) \geq 2$ if our conjecture above is true and $n \geq m+4$. This is not so far from best possible since the first two examples of section 7 both yield $\gg D^{2/m(n-1)}$. such integers $d \leq D$.

Acknowledgements. Many thanks to Lucia Caporaso, Pete Clark, Brian Conrey, Noam Elkies, Kevin James, Florian Luca, Barry Mazur, Jonathan Pila, Mark Watkins, Matt Young, and Umberto Zannier for their helpful remarks and comments on this speculative paper, and especially to Ernst Kani for his contributions to section 7. Special thanks to the extraordinary referee for his or her care over the details, presentation and content of this article, for suggesting section 11, as well as for suggesting the second example of section 7 (which was communicated as a counterexample to a conjecture in the original version of this article!).

References

[1] W. Barth, C. Peters and A. Van de Ven, *Compact complex surfaces*, Springer-Verlag, 1984.

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

[3] J. Brunier, K. James, W. Kohnen, K. Ono, C. Skinner and V. Vatsal, *Central critical values of quadratic twists of modular L-functions and some applications*, Topics in Number Theory (eds. S. Ahlgren, G. Andrews, K. Ono), Kluwer Academic, Dordrecht, Netherlands, 1999, pp. 115–125.

[4] L. Caporaso, J. Harris and B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), 1–35.

[5] H. Cohen and H.W. Lenstra Jr, *Heuristics on class groups*, Lecture Notes in Math **1052** (1984), 26–36.

[6] H. Cohen and H.W. Lenstra Jr, *Heuristics on class groups of number fields*, Lecture Notes in Math **1068** (1984), 33–62.

[7] J.B. Conrey, J. Keating, M. Rubinstein and N. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions*, Number theory for the millennium, I, (eds, M.A. Bennett et al.), A.K.Peters, Natick, MA, 2002, pp. 301–315.

[8] P. Cutter, A. Granville and T. Tucker, *The number of fields generated by the squareroot of values of a given polynomial*, Canad. Math. Bull **46** (2003), 71–79.

[9] C. Delaunay and M. Watkins, *The powers of logarithm for quadratic twists* (to appear).

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

[11] F. Gouvêa and B.y Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc **4** (1991), 1–23.

[12] A. Granville, *ABC means we can count squarefrees*, Int. Math. Res. Not **19** (1998), 991–1009.

[13] L. Holzer, *Minimal solutions of diophantine equations*, Canad. J. Math **2** (1950), 238–244.

[14] S. Lang, *Conjectured Diophantine estimates on elliptic curves*, Arithmetic and Geometry, I, vol. 35, Progr. Math., Birkhäuser Boston, Boston, Mass, 1983, pp. 155–171.

[15] K. Rubin and A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc **39** (2002), 455–474.

[16] C. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc **8** (1995), 943–973.

Département de Mathématiques et statistique, Université de Montréal, CP 6128 succ. Centre-Ville, Montréal QC H3C 3J7, Canada

E-mail address: andrew@dms.umontreal.ca