The Number of Integral Points on Arcs and Ovals

E. Bombieri and J. Pila*

1. Introduction

In 1926, Jarnik [4] proved that a strictly convex arc $y = f(x)$ of length ℓ contains at most

$$3(4\pi)^{-\frac{1}{3}}\ell^{\frac{2}{3}} + O(\ell^{\frac{1}{3}})$$

integral lattice points, and that the exponent and constant are best possible.

However, Swinnerton–Dyer [10] showed that the preceding result can be substantially improved if we start with a fixed, C^3, strictly convex arc Γ and consider the number of lattice points on $t\Gamma$, the dilation of Γ by a factor t, $t \geq 1$. This of course is the same as asking for rational points $(\frac{m}{N}, \frac{n}{N})$ on Γ as $N \to \infty$. In fact, Swinnerton–Dyer proves a bound of type

$$|t\Gamma \cap \mathbb{Z}^2| \leq c(\Gamma, \varepsilon)t^{\frac{3}{5}+\varepsilon}$$

for $\varepsilon > 0$.

A little later, W. M. Schmidt [8] gave a uniform version of Swinnerton–Dyer's Theorem (with respect to Γ) and generalized it to higher dimensions. Schmidt proved that if $f \in C^3([0, N])$ with $|f| \leq N$ and $f'''\neq 0$ in $[0, N]$, then the number of integral points on the curve $\Gamma\colon y = f(x)$ does not exceed $c(\varepsilon)N^{\frac{3}{5}+\varepsilon}$ for every $\varepsilon > 0$, for some $c(\varepsilon)$ independent of f, and conjectured the result with exponent $\frac{1}{2}$. His result and conjecture are actually more precise, but we have stated them in a modified form for the sake of simplicity.

In this paper, we obtain a result which may be considered a first step toward Schmidt's conjecture, namely, that the hypotheses $f \in C^D([0, N])$, $|f| \leq N$, $|f'| \leq 1$, $f^{(D)}\neq 0$ in $[0, N]$ imply

$$|\Gamma \cap \mathbb{Z}^2| \leq c(\varepsilon_D)N^{\frac{1}{2}+\varepsilon_D}$$

where $\varepsilon_D \to 0$ as $D \to \infty$. We prove also an independent conjecture of Sarnak [7] that if $f \in C^\infty([0, 1])$ is strictly convex then

$$|t\Gamma \cap \mathbb{Z}^2| \leq c(f, \varepsilon)t^{\frac{1}{2}+\varepsilon}$$

for every $\varepsilon > 0$. In view of the example $f(x) = \sqrt{x}$, the exponent $\frac{1}{2}$ is best possible here, and in Schmidt's conjecture. These results are proved in section 4.

If Γ is a subset of an irreducible algebraic curve of degree d inside a square of side N, we show that the number of lattice points on Γ is bounded by

$$c(d, \varepsilon)N^{\frac{1}{d}+\varepsilon}$$

for any $\varepsilon > 0$, and determine $c(d, \varepsilon)$, which is otherwise independent of Γ, explicitly. This appears to be new if $d \geq 3$. The example $f(x) = x^d$ shows that the exponent $\frac{1}{d}$ is best possible. This result is proved in section 3.

* Supported in part by NSF grant DMS 8610730.

If f is a transcendental analytic function on $[0,1]$, we prove in section 2 the bound

$$|t\Gamma \cap \mathbb{Z}^2| \leq c(f,\varepsilon)t^{\varepsilon}$$

for every $\varepsilon > 0$, answering a question implicitly raised by Sarnak [7]. The same bound holds if f is an algebraic function, unless the curve $y = f(x)$ admits a parametrization $x = X(u)$, $y = Y(u)$, by rational polynomials X, Y. The related conjecture

$$|\Gamma \cap \mathbb{Z}^2| \leq c(d,\varepsilon)N^{\varepsilon}$$

for algebraic Γ of degree d and genus ≥ 1, proposed by W. M. Schmidt, is still open due to lack of uniformity in our arguments.

Our results are sufficiently uniform that they can be extended to higher dimensions by simple slicing arguments.

We would like to thank Peter Sarnak for drawing our attention to these problems.

2. Main Lemma and Analytic Curves

Let Γ be the arc $y = f(x)$, $0 \leq x \leq N$, where $f \in C^k([0,N])$. We are interested in the integral lattice points on Γ. Let $P_1, \cdots, P_s$ be these points, arranged in order of increasing abscissae.

Let $d \geq 1$ be an integer, and define a finite sequence n_ℓ of integers as follows.

(i) $n_0 = 1$

(ii) Suppose $n_{\ell-1}$ has been defined. Then n_ℓ is the unique integer such that the points P_i for $n_{\ell-1} \leq i < n_\ell$ lie on some real algebraic curve of degree $\leq d$, but the points P_i for $n_{\ell-1} \leq i \leq n_\ell$ do not, if such an integer n_ℓ exists. Otherwise, the sequence terminates with $n_{\ell-1}$.

Suppose the sequence n_ℓ has $m+1$ elements.

Let $D = \frac{1}{2}(d+1)(d+2)$. Then any $D-1$ points in the plane lie on some curve of degree at most d. Hence $n_\ell - n_{\ell-1} \geq D-1$.

Let J_d denote the set of pairs $j = (j_1, j_2)$ with $0 \leq j_1, j_2 \leq j_1 + j_2 \leq d$. So $|J_d| = D$. If P is a point with coordinates (x,y) we write

$$P^j = P^{(j_1,j_2)} = x^{j_1}y^{j_2} \ .$$

Lemma 1. *The points $P_{n+1}, \cdots, P_{n+t}$ lie on some algebraic curve of degree $\leq d$ if and only if*

$$\operatorname{rank}\left(P_i^j\right)_{\substack{n+1\leq i\leq n+t \\ j\in J_d}} < D \ .$$

Proof. Let

$$A = \left(P_i^j\right)_{\substack{n+1\leq i\leq n+t \\ j\in J_d}} \ .$$

Suppose that

$$f(x,y) = \sum_{j\in J_d} a_j x^{j_1}y^{j_2}, \quad a_j \in \mathbb{R}$$

defines an algebraic curve of degree $\leq d$ through $P_{n+1}, \cdots, P_{n+t}$, and that $t \geq D$. Then

$$\sum_{j \in J_d} a_j P_i^j = 0$$

for $i \in I$, $I \subset \{n+1, \cdots, n+t\}$ any subset of cardinality D. Thus

$$\det \left(P_i^j \right)_{\substack{i \in I \\ j \in J_d}} = 0$$

and $\operatorname{rank}(A) < D$. Conversely, suppose that $\operatorname{rank}(A) = r < D$. Let

$$A_{IJ} = \left(P_i^j \right)_{\substack{i \in I \\ j \in J}}$$

be an $r \times r$ minor of A of maximal rank. Since $r < D$, there is a $j^* \notin J$. Let

$$f(x,y) = \det \begin{pmatrix} A_{Ij} \\ x^{j_1} y^{j_2} \end{pmatrix}_{j \in J \cup \{j^*\}} .$$

Then $f(x,y)$ has degree $\leq d$, and the cofactor of $x^{j_1^*} y^{j_2^*}$ is $\det(A_{IJ}) \neq 0$. For any i with $n+1 \leq i \leq n+t$, we have

$$f(P_i) = \det \begin{pmatrix} A_{Ij} \\ P_i^j \end{pmatrix}_{j \in J \cup \{j^*\}} = 0 ,$$

since if $i \in I$ we have two identical rows, while if $i \notin I$, the determinant is zero by definition of rank. □

Corollary.

(*i*)
$$\operatorname{rank} \left(P_i^j \right)_{\substack{n_{\ell-1} \leq i < n_\ell \\ j \in J_d}} = D - 1.$$

(*ii*)
$$\operatorname{rank} \left(P_i^j \right)_{\substack{n_{\ell-1} \leq i \leq n_\ell \\ j \in J_d}} = D .$$

Let I be a closed bounded interval. For a function $f \in C^k(I)$ we define

$$\|f\|_{N,k} = \max_{\substack{\kappa \leq k \\ x \in I}} N^{\kappa - 1} \frac{|f^{(\kappa)}(x)|}{\kappa!} .$$

We remark that this norm is invariant under dilations, meaning that if $f \in C^k(I)$, and f_t is defined by

$$f_t(x) = t f\left(\frac{x}{t}\right)$$

then $f_t \in C^k(tI)$ and

$$\|f_t\|_{tN,k} = \|f\|_{N,k} .$$

Also $\|x\|_{N,k} = 1$ for $I \subset [0, N]$.

Proposition 1. *Suppose $f_1, \cdots, f_m \in C^k(I)$. Then*

$$\|f_1 \cdots f_m\|_{N,k} \leq ((k+1)N)^{m-1} \|f_1\|_{N,k} \cdots \|f_m\|_{N,k} \ .$$

In particular

$$\|x^p f^q\|_{N,k} \leq ((k+1)N)^{p+q-1} \|f\|_{N,k}^q \ ,$$

for $I \subseteq [0, N]$ and positive integers p, q.

Proof. For any $\kappa \leq k$,

$$\frac{d^\kappa}{dx^\kappa}(f_1 \cdots f_m) = \sum_{i_1+\cdots+i_m=\kappa} \frac{\kappa!}{i_1! \cdots i_m!} f_1^{(i_1)} \cdots f_m^{(i_m)} \ .$$

Hence for any $x \in I$,

$$\begin{aligned} N^{\kappa-1}(\kappa!)^{-1} &|\frac{d^\kappa}{dx^\kappa}(f_1 \cdots f_m)(x)| \\ &\leq N^{\kappa-1} \sum_{i_1+\cdots+i_m=\kappa} N^{m-\kappa} \prod_{j=1}^m N^{i_j-1}(i_j!)^{-1} |f_j^{(i_j)}(x)| \\ &\leq N^{m-1}(\kappa+1)^{m-1} \|f_1\|_{N,\kappa} \cdots \|f_m\|_{N,\kappa} \ . \ \square \end{aligned}$$

We now need the following identity. Let x, x_i, y_{ij} for $i, j = 1, \cdots, n$ be indeterminates, and let $V(x_1, \cdots, x_k)$ denote the van der Monde determinant. Define

$$g_{ij}(x) = \frac{-1}{V(x_1, \cdots, x_i)} \det \begin{pmatrix} 1 & x_1 & \dots & x_1^{i-1} & y_{1j} \\ & \vdots & & & \\ 1 & x_i & \dots & x_i^{i-1} & y_{ij} \\ 1 & x & \dots & x^{i-1} & 0 \end{pmatrix} .$$

Note that, for an indeterminate y,

$$g_{ij}(x) = \frac{-1}{V(x_1, \cdots, x_i)} \det \begin{pmatrix} 1 & x_1 & \dots & x_1^{i-1} & y_{1j} \\ & \vdots & & & \\ 1 & x_i & \dots & x_i^{i-1} & y_{ij} \\ 1 & x & \dots & x^{i-1} & y \end{pmatrix} + y \ ,$$

so that $g_{ij}(x)$ is the unique polynomial in x of degree $i-1$ with $g_{ij}(x_k) = y_{kj}$ for $k = 1, \cdots, i$. We write $g_{ij}^{(\ell)}$ for $(\frac{d}{dx})^\ell g_{ij}$.

Proposition 2. *With the above definitions,*

$$\det(y_{ij}) = \frac{V(x_1, \cdots, x_n)}{1! \dots (n-1)!} \det \left(g_{ij}^{(i-1)} \right) \ .$$

Proof. The proof is by evaluation of the right-hand side. Differentiating g_{ij} by rows we get

$$\frac{V(x_1,\cdots,x_n)}{1!\dots(n-1)!}\det\left(g_{ij}^{(i-1)}\right)$$

$$=\frac{V(x_1,\cdots,x_n)}{1!\dots(n-1)!}\det\left(\frac{-1}{V(x_1,\cdots,x_i)}\det\begin{pmatrix}1 & x_1 & \dots & x_1^{i-1} & y_{1j}\\ & \vdots & & & \\ 1 & x_i & \dots & x_i^{i-1} & y_{ij}\\ 0 & 0 & \dots & (i-1)! & 0\end{pmatrix}\right)$$

$$=\frac{V(x_1,\cdots,x_n)}{V(x_1,x_2)\dots V(x_1,\cdots,x_n)}\det\left(\det\begin{pmatrix}1 & x_1 & \dots & x_1^{i-2} & y_{1j}\\ & \vdots & & & \\ 1 & x_i & \dots & x_i^{i-2} & y_{ij}\end{pmatrix}\right)$$

$$=\frac{1}{V(x_1,x_2)\dots V(x_1,\cdots,x_{n-1})}\det\left(\sum_{k=1}^{i}(-1)^{k-i}V(x_1,\cdots,\hat{x}_k,\cdots,x_i)y_{kj}\right)$$

where the $\hat{}$ denotes an omitted variable. We express this last matrix as a product of a lower triangular matrix and the matrix (y_{ij}) to obtain the expression

$$\frac{1}{V(x_1,x_2)\dots V(x_1,\cdots,x_{n-1})}\det\begin{pmatrix}&&&\bigcirc\\ &&\ddots&\\ (-1)^{i-j}V(x_1,\cdots,\hat{x}_j,\cdots,x_i)&&&\end{pmatrix}\det(y_{ij})$$

$$=\frac{1}{V(x_1,x_2)\dots V(x_1,\cdots,x_{n-1})}\cdot\prod_{k=1}^{n-1}V(x_1,\cdots,x_k)\cdot\det(y_{ij})$$

$$=\det(y_{ij})\ .\ \square$$

In what follows I denotes a closed subinterval of $[0,N]$, and we write $\|\ \|_k$ for $\|\ \|_{N,k}$. We apply the preceding proposition choosing $y_{ij}=f_j(x_i)$, where $x_1,\cdots,x_n\in I$ are distinct points and $f_j\in C^{n-1}(I)$. Then the mean value theorem shows that $g_{ij}^{(i-1)}$ is in the range of $f_j^{(i-1)}$ (see for example Swinnerton–Dyer [10], Lemma 1, p. 131, or Posse [6]). By expanding $\det(g_{ij}^{(i-1)})$ we get

$$|\det(f_j(x_i))|\le|V(x_1,\cdots,x_n)|n!\max_\sigma\prod\sup\frac{1}{(i-1)!}|\frac{d^{i-1}}{dx^{i-1}}f_{\sigma(i)}(x)|$$

for σ running over permutations of $\{1,\cdots,n\}$. A direct proof of this result could also be obtained by appealing to a mean value theorem of H.A.Schwarz ([9], Zw. Bd., p. 300). In view of the definition of norms $\|\ \|_k$, this yields a fortiori

$$|\det(f_j(x_i))|\le|V(x_1,\cdots,x_n)|n!N^{-\frac{n(n-3)}{2}}\|f_1\|_{n-1}\dots\|f_n\|_{n-1}\ . \tag{1}$$

Lemma 2. *For the sequence $n_0, \cdots, n_m$ associated to the curve $\Gamma:\ y = f(x)$, $x \in I$, $f \in C^{D-1}(I)$, and any integer $d \geq 1$ we have*

$$|x_{n_{\ell+1}} - x_{n_\ell}| \geq \left(D^2 \|f\|_{D-1}\right)^{-\frac{4}{3(d+3)}} N^{1-\frac{8}{3(d+3)}} \ .$$

Proof. By lemma 1, the matrix

$$\left(P_i^j\right)_{\substack{n_\ell \leq i \leq n_{\ell+1} \\ j \in J_d}}$$

has maximal rank D. Thus there is a subset $I \subset \{n_\ell, \cdots, n_{\ell+1}\}$ of cardinality D (no confusion should arise with the interval I of definition of f) such that

$$\Delta = \det\left(P_i^j\right)_{\substack{i \in I \\ j \in J_d}} \neq 0 \ .$$

Obviously Δ is an integer, which gives $|\Delta| \geq 1$. We now use formula (1) appropriately to give an upper bound for $|\Delta|$. We apply (1) with $n = D$, the points x_i with $i \in I$ and f_j the functions $x^{j_1} f(x)^{j_2}$ for $(j_1, j_2) \in J_d$ in some order. Clearly,

$$|V(x_i; i \in I)| \leq |x_{n_{\ell+1}} - x_{n_\ell}|^{\frac{D(D-1)}{2}} \ .$$

Hence (1) yields:

$$\begin{aligned}
|\Delta| &\leq |x_{n_{\ell+1}} - x_{n_\ell}|^{\frac{D(D-1)}{2}} N^{-\frac{D(D-3)}{2}} D! \prod_{j \in J_d} \|x^{j_1} f(x)^{j_2}\|_{D-1} \\
&\leq |x_{n_{\ell+1}} - x_{n_\ell}|^{\frac{D(D-1)}{2}} N^{-\frac{D(D-3)}{2}} D^D \prod_{j \in J_d} (DN)^{j_1+j_2-1} \|f\|_{D-1}^{j_2} \\
&= \left(\frac{|x_{n_{\ell+1}} - x_{n_\ell}|}{N}\right)^{\frac{D(D-1)}{2}} (DN)^{\frac{dD}{3}} \|f\|_{D-1}^{\frac{dD}{6}}
\end{aligned}$$

Since $|\Delta| \geq 1$, the lemma follows after some simplification. □

Since $D^{\frac{8}{3(d+3)}} < 3$ for every d, the following is now obvious:

Main Lemma. *Let $d \geq 1$, $D = \frac{1}{2}(d+1)(d+2)$ and $f \in C^{D-1}(I)$. Then the integral points on $\Gamma:\ y = f(x)$, $x \in I$ lie on the union of not more than*

$$3\left(\|f\|_{D-1}^{\frac{1}{2}} N\right)^{\frac{8}{3(d+3)}} + 1$$

real algebraic curves of degree $\leq d$. If $\|f\|_{D-1}^{\frac{1}{2}} N \geq 1$, this in turn does not exceed

$$4\left(\|f\|_{D-1}^{\frac{1}{2}} N\right)^{\frac{8}{3(d+3)}} \ .$$

Remark. Our construction shows that the curves can be taken to be defined over $\mathbb{Z}$, with height at most

$$D!\left(N^2 \|f\|_0\right)^{\frac{dD}{3}} \ ,$$

but we have no use for this fact in the sequel.

We can now prove

Theorem 1. *Let $f(x)$ be a real analytic function on a closed bounded interval I and suppose that $f(x)$ is not algebraic. Let Γ be the graph of $f(x)$. Let $\varepsilon > 0$. Then there is a constant $c(f, \varepsilon)$ such that*

$$|t\Gamma \cap \mathbb{Z}^2| \leq c(f, \varepsilon) t^{\varepsilon}$$

for all $t \geq 1$.

Proof. Without loss of generality, we may assume $I \subseteq [0, 1]$. Since Γ is compact and $f(x)$ is not algebraic, Γ intersects any algebraic curve in only finitely many points. Since the space of algebraic curves of a given degree d is compact, there is a number $\gamma(f, d)$ such that Γ intersects any algebraic curve of degree d in at most $\gamma(f, d)$ points. Combining with the Main Lemma and using the scaling invariance of the norm, we find that

$$|t\Gamma \cap \mathbb{Z}^2| \leq \gamma(f, d) \left\{ \|f\|_{I, D-1}^{\frac{4}{3(d+3)}} t^{\frac{8}{3(d+3)}} + 1 \right\} . \square$$

We remark that the numbers $\gamma(f, d)$, for a given f, can grow in an arbitrary manner. Consider, for example,

$$f(x) = \sum_{i=0}^{\infty} 2^{-d_i} \prod_{k=1}^{d_i} (x - 2^{-k}) .$$

This $f(x)$ is analytic in the unit disk, and

$$\gamma(f, d_i) \geq d_{i+1} .$$

We now show that if $f(x)$ is algebraic, the conclusion of the above Theorem continues to hold unless Γ admits a parametrization by rational polynomials. Let $\tau(n)$ denote the number of divisors of the integer n.

Theorem 2. *Let $F(x, y) \in \mathbb{R}[x, y]$ be the defining equation of a real algebraic irreducible plane curve C. Then the number of rational points $\left(\frac{m}{N}, \frac{n}{N}\right)$ with $|m|, |n| \leq N$ on C does not exceed*

$$O\left(\tau(N)^a (\log\ N)^b\right)$$

with $a = a(C)$, $b = b(C)$, except in the case in which C admits a rational polynomial parametrization.

Proof. Without loss of generality, we may assume that C is defined over $\mathbb{Q}$. If the curve C has genus $g \geq 1$ then the number of rational points P of logarithmic height $h(P) \leq H$ is bounded by $c_0(C, \varepsilon) H^{r+\varepsilon}$, where $r = \text{rank}\ J(\mathbb{Q})$ is the rank of the Mordell–Weil group of the Jacobian J of C (there is no need to invoke here the well-known theorem of Faltings that $|C(\mathbb{Q})| < \infty$ if $g \geq 2$, the above weaker result being amply sufficient for our modest needs). This shows that the number of rational points $\left(\frac{m}{N}, \frac{n}{N}\right)$ with $m, n = O(N)$ on C is $O((\log\ N)^{c_1})$ for some $c_1 > 0$ if C has geometric genus ≥ 1.

Now suppose that C has geometric genus 0. Then C is rational and either $|C(\mathbb{Q})| < +\infty$ or C has a non-singular rational point. By a result of Hilbert and Hurwitz [3] it then

follows in the latter case that C has a birational parametrization $x = x(t)$, $y = y(t)$ with $x(t), y(t)$ rational functions in $\mathbb{Q}(t)$, and we can write

$$x(t) = \frac{p(t)}{r(t)}, \qquad y(t) = \frac{q(t)}{r(t)},$$

where $p, q, r \in \mathbb{Z}[t]$ and $GCD(p, q, r) = 1$. Moreover $t = T(x(t), y(t))$ for some $T \in \mathbb{Q}(x, y)$, therefore all rational points of C come from rational values of t. We want to solve

$$\frac{p(t)}{r(t)} = \frac{m}{N}, \qquad \frac{q(t)}{r(t)} = \frac{n}{N}$$

or equivalently

$$Np(t) = mr(t), \qquad Nq(t) = nr(t). \tag{2}$$

Since $GCD(p, q, r) = 1$ there are polynomials $A(t), B(t), C(t)$ in $\mathbb{Z}[t]$ such that

$$A(t)p(t) + B(t)q(t) + C(t)r(t) = d$$

for some integer d, identically in t. Thus

$$A(t)Np(t) + B(t)Nq(t) + C(t)Nr(t) = dN$$

so equation (2) becomes

$$(mA(t) + nB(t) + NC(t))r(t) = dN \tag{3}$$

to be solved for rational t.

Let $r(t) = r_0t^k + r_1t^{k-1} + \cdots + r_k$ and let $t = u/v$. Then (3) implies

$$r_0u^k + r_1u^{k-1}v + \cdots + r_kv^k \mid dNv^{k'}$$

for some k'. Now $(u, v) = 1$ and

$$\begin{aligned}(r_0u^k + r_1u^{k-1}v + \cdots + r_kv^k, v^{k'}) &\mid (r_0u^k + r_1u^{k-1}v + \cdots + r_kv^k, v)^{k'} \\ = (r_0u^k, v)^{k'} &= (r_0, v)^{k'} \mid r_0^{k'},\end{aligned}$$

and we get

$$r_0u^k + r_1u^{k-1}v + \cdots + r_kv^k \mid dr_0^{k'}N. \tag{4}$$

If $r(t)$ has at least 3 distinct roots, (4) is a Thue–Mahler equation and the number of solutions does not exceed c_2^w, where w is the number of distinct prime factors of $dr_0^{k'}N$ and c_2 depends only on the degree k and the coefficients r_i, by an old result of Lewis and

Mahler [5] (we can take c_2 a power of k, independent of the r_i's, but we do not need this more difficult result). Thus in this case we have only $O(\tau(N)^{c_3})$ solutions.

Suppose now that r has not more than two distinct roots, hence

$$r(t) = r_0(t-\alpha)^k$$

or

$$r(t) = r_0(t-\alpha)^\ell(t-\beta)^{k-\ell}$$

with $\alpha, \beta \in \mathbb{Q}$, or

$$r(t) = r_0((t-\alpha)(t-\overline{\alpha}))^{k/2}$$

with α of degree 2 over $\mathbb{Q}$ and k even.

If $r(t) = r_0(t-\alpha)^\ell(t-\beta)^{k-\ell}$ then by (4) we deduce that $r_0u - r_0\alpha v$ and $r_0u - r_0\beta v$ divide $dr_0^{k'}N$, which gives at most $(2\tau(dr_0^{k'}N))^2$ solutions (u,v).

If instead $r(t) = r_0((t-\alpha)(t-\overline{\alpha}))^{k/2}$ then

$$r_0(u-\alpha v)(u-\overline{\alpha}v) \mid dr_0^{k'}N. \tag{5}$$

If the quadratic form in (5) is definite, the preceding argument still gives a power of a divisor function for the number of solutions. If however the quadratic form is indefinite, the quadratic field $\mathbb{Q}(\alpha)$ is real and the above argument works only up to units in a suitable localization of $\mathbb{Z}[\alpha]$. In any case, one sees that the number of solutions of (5) with $|u|, |v| \le X$ is bounded by $O(\tau(N)^{c_4}(\log X)^{c_5})$ for some constants c_4, c_5 depending on α. Since the parametrization $(x(t), y(t))$ is birational we can write $t = T(x(t), y(t))$ for some $T \in \mathbb{Q}(x,y)$, which shows that if $(x,y) = (\frac{m}{N}, \frac{n}{N})$ with $m, n = O(N)$ then $u, v = O(N^{c_6})$ for some c_6. Hence in this case we cannot have more than $O(\tau(N)^{c_4}(\log N)^{c_5})$ solutions.

It remains for consideration the case in which $r(t) = r_0(t-\alpha)^k$. After a translation in t, we may assume that $\alpha = 0$ and

$$r(t) = r_0t^k.$$

If $k \ge 1$ then (4) implies that $u \mid dr_0^{k'}N$. If $p = \deg p(t) > k$, then $x = \frac{p(t)}{r(t)} = \frac{m}{N}$ implies also that $v \mid dr_0^{k'}N$, and we get at most $O(\tau(N)^2)$ solutions. The same argument of course can be applied to the y coordinate, so that we remain with $\deg_t x(t) \le 0$, $\deg_t y(t) \le 0$. However, in this last case we have $x(t) = r_0^{-1}t^{-k}p(t)$, $y(t) = r_0^{-1}t^{-k}q(t)$ with $p(t), q(t)$ polynomials of degree $\le k$. By reparametrizing C by means of $t \to t^{-1}$ we see that the only case left is the case in which $k = 0$. Hence C is parametrized by polynomials. □

Combining the previous two theorems we get the following result.

Theorem 3. *Suppose $\phi\colon S^1 \to \mathbb{R}^2$ is analytic. Then for all $\varepsilon > 0$*

$$|t\phi(S^1) \cap \mathbb{Z}^2| \le c(\phi, \varepsilon)t^\varepsilon \ .$$

Proof. If the image $\phi(S^1)$ is algebraic, it clearly cannot be parametrized by polynomials, so the conclusion follows from the stronger Theorem 2. If $\phi(S^1)$ is not algebraic, we can use the finite number of points where the tangent to $\phi(S^1)$ has slope ± 1 to divide $\phi(S^1)$ into finitely many pieces, each an analytic function with respect to one of the coordinate axes. The conclusion then follows from Theorem 1. □

In particular, the estimate $c(\Omega,\varepsilon)t^{\varepsilon}$ holds for the number of integer points on the dilation by a factor t of a real analytic oval Ω.

We remark that the conclusion can fail if ϕ is not analytic at just one point. As an example of this, consider the curve

$$C\colon y^2 = x^2(x+1)\ .$$

The curve C admits a parametrization

$$x = u^2 - 1\ , \qquad y = u^3 - u\ ,$$

giving a map $[-1,1] \to C$ which, considered as a map $\phi\colon S^1 \to \mathbb{R}^2$ is continuous and analytic except at $u = \pm 1$. However, considering the points

$$x = -\frac{n(n^2-k^2)}{n^3}, \qquad y = \frac{k(n^2-k^2)}{n^3}, \qquad k = -n, \cdots, n-1$$

we see that (setting $t = n^3$)

$$|t\phi(S^1) \cap \mathbb{Z}^2| \geq 2t^{\frac{1}{3}}\ .$$

3. Integral Points on Algebraic Curves

Our object in this section is to obtain a bound for the number of integral solutions in a square of side N to an equation of the form

$$F(x,y) = 0$$

where $F(x,y) \in \mathbb{R}[x,y]$ is irreducible of degree $d \geq 2$. We follow the same approach as in section 2. In order to preclude the possibility that the algebraic curves we construct may contain the curve $F(x,y) = 0$ as a component, we will restrict the monomials used to define them. We thus begin by developing a general form of the Main Lemma of the previous section.

Let M be a finite set of monomials in the indeterminates x and y, and let D be the cardinality of M. Set also

$$J = \left\{j = (j_1, j_2)\colon x^{j_1}y^{j_2} \in M\right\}$$
$$p = \sum_{j\in J}(j_1 + j_2)\ , \qquad q = \sum_{j\in J} j_2\ .$$

Suppose C is an algebraic curve defined by $G(x,y) = 0$ where $G(x,y) \in \mathbb{R}[x,y]$. We will say that C is defined in M if the monomials appearing in G all belong to M.

Again, let I be a closed subinterval of $[0,N]$ and suppose that Γ is the graph of $y = f(x)$ for $x \in I$, where $f \in C^{D-1}(I)$.

Let $P_1, \cdots, P_s$ be the integral points of Γ, arranged in order of increasing abscissae. Define a finite sequence n_ℓ as follows:

(i) $n_0 = 1$.

(ii) Suppose n_ℓ has been defined. Then $n_{\ell+1}$ is the unique integer such that the points P_i for $n_\ell \leq i < n_{\ell+1}$ lie on an algebraic curve defined in M, but the points P_i for $n_\ell \leq i \leq n_{\ell+1}$ do not, if such an integer $n_{\ell+1}$ exists. Otherwise the sequence terminates with n_ℓ.

Lemma 3. *The points $P_{n+1}, \cdots, P_{n+t}$ lie on some algebraic curve defined in M if and only if*

$$\text{rank } \left(P_i^j\right)_{\substack{n+1\le i\le n+t \\ j\in J}} < D \ .$$

Proof. The proof is completely analogous to the proof of Lemma 1. □

Corollaries.

(*i*) $$n_{\ell+1} - n_\ell \ge D-1.$$

(*ii*) $$\text{rank } \left(P_i^j\right)_{\substack{n_\ell\le i< n_{\ell+1} \\ j\in J}} = D-1.$$

(*iii*) $$\text{rank } \left(P_i^j\right)_{\substack{n_\ell\le i\le n_{\ell+1} \\ j\in J}} = D.$$

Lemma 4. *For the sequence $n_0, \cdots, n_m$ we have*

$$|x_{n_{\ell+1}} - x_{n_\ell}| \ge \left(D^p \|f\|_{D-1}^q\right)^{-\frac{2}{D(D-1)}} N^{1-\frac{2p}{D(D-1)}}$$

Proof. The proof is entirely analogous to the proof of Lemma 2. □

As before we now obtain

Generalized Main Lemma. *Let M be a finite set of monomials in x and y. Define D, J, p, q as above. Suppose Γ is the graph of $y = f(x)$ for $x \in I$, where $f \in C^{D-1}(I)$. Then the integral points of Γ lie on the union of not more than*

$$\left(D^p \|f\|_{D-1}^q\right)^{\frac{2}{D(D-1)}} N^{\frac{2p}{D(D-1)}} + 1$$

real algebraic curves defined in M.□

When $\|f\|_{D-1}^{q/p} N \ge 1$ it is more convenient to use the bound

$$2\left(D^p \|f\|_{D-1}^q\right)^{\frac{2}{D(D-1)}} N^{\frac{2p}{D(D-1)}} \ .$$

To treat the curve $F(x,y) = 0$ we define, for each δ, a set $M_F(\delta)$ of monomials of degree $\le \delta$ in such a way that no curve defined in $M_F(\delta)$ contains the curve C determined by $F(x,y) = 0$. Let $j_F \in J_d$ be the index of the monomial of degree d of highest degree in y appearing in F. Now let δ be a positive integer, and define

$$M_F(\delta) = \left\{x^{j_1} y^{j_2} \colon d \le j_1 + j_2 \le \delta \text{ and } (x,y)^{j_F} \not| (x,y)^j\right\} \ .$$

The restriction that the monomials in $M_F(\delta)$ have degree at least d, which slightly weakens our results, is made in order to simplify our calculations.

Proposition 3. *Let $G(x,y) \in \mathbb{R}[x,y]$ and suppose that the monomials appearing in G all belong to $M_F(\delta)$. Then*

$$F(x,y) \not| G(x,y) \ .$$

Hence, by Bézout's theorem, the curves determined by F and G intersect in at most $d\delta$ points.

Proof. Suppose that, contrary to the proposition,

$$G(x,y) = H(x,y)F(x,y)$$

for some $H(x,y) \in \mathbb{R}[x,y]$. Then the monomial $(x,y)^{j_H}(x,y)^{j_F}$ appears in $G(x,y)$, contradicting the hypothesis that all the monomials in G belong to $M_F(\delta)$ and are not divisible by $(x,y)^{j_F}$. $\square$

We now fix $F(x,y)$ and δ, and assume that $\delta \geq 2d$. We let $M = M_F(\delta)$, and define D, J, p, q as before.

For $h \geq d$, the number of monomials of exact degree h not divisible by a fixed monomial of degree d is d. Thus we have:

$$\begin{aligned} D &= d(\delta - d + 1) \ , \\ p &= d[\frac{1}{2}\delta(\delta+1) - \frac{1}{2}d(d-1)] \ . \end{aligned}$$

and

$$\begin{aligned} \frac{2p}{D(D-1)} &= \frac{d[\delta(\delta+1) - d(d-1)]}{d(\delta-d+1)[d(\delta-d+1)-1]} \\ &= \frac{[\delta-(d-1)](\delta+d)}{(\delta-d+1)[d(\delta-d+1)-1]} = \frac{\delta+d}{d\delta - d^2 + d - 1} \ . \end{aligned}$$

We also note that

$$\begin{aligned} \frac{1}{d} \leq \frac{1}{d}\left(\frac{\delta+d}{\delta+1}\right) &= \frac{\delta+d}{d\delta+d} \leq \frac{2p}{D(D-1)} \\ &\leq \frac{\delta+d}{d\delta-d^2} = \frac{1}{d}\left(\frac{\delta+d}{\delta-d}\right) \leq \frac{1}{d} + \frac{2}{\delta-d} \\ &\leq \frac{1}{d} + \frac{4}{\delta} \end{aligned}$$

since $\delta - d \geq \frac{1}{2}\delta$.

We now consider a C^∞ function $f(x)$ on a closed interval $I \subseteq [0,N]$ with $F(x,f) = 0$ and $|f'(x)| \leq 1$. Since the graph of f intersects any curve defined in M in at most $d\delta$ points, by applying the Generalized Main Lemma we find that the graph of f contains at most

$$d\delta\left[\left(D^p \|f\|_{D-1}^q\right)^{\frac{2}{D(D-1)}} N^{\frac{2p}{D(D-1)}} + 1\right]$$

integral points. Our next objective is to obtain a bound independent of the norms of f, essentially by showing that the intervals on which the norms are large, are small.

Lemma 5. *Suppose $G(x,y) \in \mathbb{R}[x,y]$ is absolutely irreducible and of degree b. Let $g(x)$ be a C^∞ function on an interval I, with $G(x,g) = 0$. Suppose $g(x)$ is not a polynomial. Then for $k \geq 1$ and $c \in \mathbb{R}$, the equation*

$$g^{(k)}(x) = c$$

has at most $b(b-1)(2k-1)$ solutions $x \in \mathbb{R}$.

Proof. Since $G(x,g) = 0$ we have by differentiation that

$$G_x + G_y g' = 0 \ . \tag{6}$$

Now suppose that

$$H_k + G_y^{a_k} g^{(k)} = 0 \tag{7}$$

and let $h_k = \deg(H_k)$. Then

$$H_{kx} + H_{ky}g' + a_k G_y^{a_k - 1}(G_{yx} + G_{yy}g')g^{(k)} + G_y^{a_k} g^{(k+1)} = 0 \ .$$

Multiplying by G_y^2 and substituting using (6) and (7) we obtain

$$G_y(H_{kx}G_y - H_{ky}G_x) - a_k H_k(G_{yx}GG_y - G_{yy}G_x) + G_y^{a_k+2} g^{(k+1)} = 0 \ .$$

For the sequences a_k and h_k we therefore have the following recurrences:

$$\left.\begin{array}{c} a_{k+1} = a_k + 2 \\ a_1 = 1 \end{array}\right\} a_k = 2k - 1$$

$$\left.\begin{array}{c} h_{k+1} \leq h_k + 2b - 3 \\ h_1 = b - 1 \end{array}\right\} h_k \leq (2k-1)(b-1) - k$$

and solutions of $g^{(k)}(x) = c$ are among the values of x corresponding to the intersection of the two curves

$$G(x,y) = 0 \ , \qquad H_k + G_y^{a_k} c = 0 \ .$$

Since g is not a polynomial, $g^{(k)}$ is not identically equal to any constant, and since G is irreducible, the intersection is proper and consists of at most

$$b(b-1)(2k-1)$$

points as claimed. □

Lemma 6. *Let $g(x)$ be a C^∞ function on an interval I, satisfying $G(x,g) = 0$, where $G(x,y) \in \mathbb{R}[x,y]$ is irreducible of degree $b \geq 2$. Let A_ℓ be positive real numbers for $\ell = 1, \cdots, k$. Then we can divide I into at most $2b^2k^2$ subintervals I_ν such that for each ν and each $\ell = 1, \cdots, k$ we have either (i) or (ii) holding:*

(*i*) $$|g^{(\ell)}(x)| \leq A_\ell \quad \textit{for all} \quad x \in I_\nu.$$

(*ii*) $$|g^{(\ell)}(x)| \geq A_\ell \quad \textit{for all} \quad x \in I_\nu.$$

Proof. If $g(x)$ is not a polynomial, we take as division points the solutions of

$$g^{(i)}(x) = \pm A_i \qquad\qquad i = 1, \cdots, k \ .$$

According to Lemma 5, there are at most

$$\sum_{i=1}^{k} 2b(b-1)(2i-1) = 2b(b-1)k^2$$

such points, giving rise to at most

$$2b(b-1)k^2 + 1 \leq 2b^2k^2$$

intervals. If $g(x)$ is a polynomial of degree at most b, we take as division points the solutions of

$$g^{(i)}(x) = \pm A_i \qquad\qquad i = 1, \cdots, b-1 \ ,$$

a total of at most

$$\sum_{i=1}^{b-1} 2(b-i) = 2b(b-1) - b(b-1) = b(b-1)$$

points.□

Lemma 7. *Suppose $I = [a,b]$, $g \in C^k([a,b])$ and for some A, N we have*

$$|g^{(i)}(x)| \leq i! A^{i/k} N^{1-i} \quad \textit{for } x \in I, \ i = 0, \cdots, k-1$$

and

$$|g^{(k)}(x)| \geq k! A N^{1-k} \quad \textit{for } x \in I \ .$$

Then $|I| \leq 2A^{-1/k}N$.

Proof. For some $\xi \in I$ we have

$$g(b) - g(a) = \sum_{i=1}^{k-1} \frac{g^{(i)}(a)}{i!}(b-a)^i + \frac{g^{(k)}(\xi)}{k!}(b-a)^k \ .$$

Hence

$$|I|^k A N^{1-k} \leq \sum_{i=1}^{k-1} |I|^i A^{i/k} N^{1-i} + 2N \ .$$

Let $\lambda = (|I|/N)A^{-1/k}$. Then we have

$$\lambda^k \leq \sum_{i=1}^{k-1} \lambda^i + 2 \ .$$

Hence $\lambda \leq 2$, completing the proof. □

We are now ready to prove

Theorem 4. *Let $f(x)$ be a C^∞ function on a closed subinterval of $[0, N]$, and suppose that $F(x, f) = 0$, where $F(x, y) \in \mathbb{R}[x, y]$ is absolutely irreducible of degree $d \geq 2$. Suppose that $|f'(x)| \leq 1$. Then the number of integral points on the graph of f is at most*

$$N^{\frac{1}{d}} \exp\left(11\sqrt{d\ \log N\ \log\log N}\right)$$

provided $N \geq \exp(d^6)$.

Proof. Let

$$G(N) = G(d, N)$$

be the maximum number of integral points on the graph of a C^∞ function $g(x)$, on an interval I of length at most N, with $|g'(x)| \leq 1$, and g satisfying some algebraic relation $G(x, g) = 0$, with G absolutely irreducible of degree d. Clearly we may assume $I \subset [0, N]$.

Now fix some $\delta \geq 2d$, and let $g(x)$ be such a C^∞ function. Given $A \geq 1$, by appealing to Lemma 6 we can divide the domain I of $g(x)$ into at most

$$2d^2(D-1)^2 \leq 2d^2D^2$$

subintervals I_ν such that for each I_ν and each $\ell = 1, \cdots, D-1$, either (i) or (ii) holds:

(i) $$|g^{(\ell)}(x)| \leq \ell! A^{\ell/(D-1)} N^{1-\ell} \quad \text{for all } x \in I_\nu$$

(ii) $$|g^{(\ell)}(x)| \geq \ell! A^{\ell/(D-1)} N^{1-\ell} \quad \text{for all } x \in I_\nu.$$

After translating the graph of $g(x)$ on each I_ν by an integer, we can assume, since $|g'(x)| \leq 1$, that

$$|g(x)| \leq N \quad \text{for all} \quad x \in I_\nu\ .$$

Now for each I_ν, either (i) or (ii) holds:

(i) $$|g^{(\ell)}(x)| \leq \ell! A^{\ell/(D-1)} N^{1-\ell} \quad \text{for all } x \in I_\nu \quad \text{and all } \ell = 0, \cdots, D-1\ .$$

In this case, $\|g\|_{D-1} \leq A$.

(ii) $$\begin{aligned} &|g^{(\ell)}(x)| \leq \ell! A^{\ell/(D-1)} N^{1-\ell} \quad \text{for all } x \in I_\nu \ \text{ and all } \ell < k\ , \text{ and} \\ &|g^{(k)}(x)| \geq k! A^{k/(D-1)} N^{1-k} \quad \text{for all } \ x \in I_\nu\ . \end{aligned}$$

In this case, the hypotheses of Lemma 7 hold with $A^{k/(D-1)}$ in place of A, and hence $|I_\nu| \leq 2A^{-\frac{1}{D-1}} N$.

For the I_ν of the first type, we apply the Generalized Main Lemma, using the set of monomials

$$M = M_{G_\nu}(\delta)$$

where G_ν is the appropriate translation of G, while if I_ν is of the second type we have $|I_\nu| \le 2A^{-\frac{1}{D-1}}N$, as noted earlier. We thus obtain the following recurrence relation for $G(N)$:

$$G(N) \le 2d^2D^2 2d\delta (D^pA^q)^{\frac{2}{D(D-1)}} N^{\frac{2p}{D(D-1)}} + 2d^2D^2 G\left(2A^{-\frac{1}{D-1}}N\right) .$$

Using $D \le d\delta$, we can write

$$G(N) \le HN^\alpha + KG(\lambda N)$$

where

$$\begin{aligned} H &= 4d^5\delta^3 (D^pA^q)^{\frac{2}{D(D-1)}} \\ K &= 2d^4\delta^2 \\ \alpha &= \frac{2p}{D(D-1)}, \quad \frac{1}{d} \le \alpha \le \frac{1}{d} + \frac{4}{\delta} \\ \lambda &= 2A^{-\frac{1}{D-1}} \ ; \end{aligned}$$

continuing, we find that, provided $\lambda^{n-1}N \ge 1$,

$$G(N) \le HN^\alpha (1 + K\lambda^\alpha + \cdots + (K\lambda^\alpha)^{n-1}) + K^n G(\lambda^n N) .$$

We now choose λ so that

$$K\lambda^\alpha = \frac{1}{2}$$

that is, we set

$$\lambda = \left(\frac{1}{2K}\right)^{1/\alpha} = (4d^4\delta^2)^{-\frac{D(D-1)}{2p}}$$

and thus

$$A = \left(\frac{2}{\lambda}\right)^{D-1} = 2^{D-1}(4d^4\delta^2)^{\frac{D(D-1)^2}{2p}} > 1 .$$

Finally, we choose n so that

$$\frac{\lambda}{N} \le \lambda^n < \frac{1}{N} .$$

Then $G(\lambda^n N) \le 1$, and

$$G(N) \le 2HN^\alpha + 2^{-n}\lambda^{-\alpha}N^\alpha \le 2(H+K)N^\alpha .$$

Our final task is to choose δ. Since $p \le q$, we have

$$\begin{aligned} H + K &\le 5d^5\delta^3(DA)^{\frac{2p}{D(D-1)}} \\ &\le 5d^5\delta^3(D2^{D-1})^{\frac{2p}{D(D-1)}}(4d^4\delta^2)^{D-1} \\ &\le 5d\delta.d^2\delta^2.(16d^4\delta^2)^D \\ &\le (d^4\delta^5)^{d\delta} \\ &\le \frac{1}{2}\delta^{9d\delta} \ . \end{aligned}$$

Hence

$$G(N) \le N^{\frac{1}{d}} \exp\left(\frac{4}{\delta}\log\ N + 9d\delta\log\ \delta\right) \ .$$

Take

$$\delta = \sqrt{4\log\ N/d\log\log\ N} \ .$$

Then $\delta \ge 2d$ provided $N \ge \exp(d^6)$ and

$$G(N) \le N^{\frac{1}{d}} \exp\left(11\sqrt{d\ \log\ N\ \log\log\ N}\right) \ .\Box$$

Theorem 5. *Let C be an absolutely irreducible curve of degree $d \ge 2$ and let $N \ge \exp(d^6)$. Then the number of integral points on C and inside a square $[0,N]\times[0,N]$ does not exceed*

$$N^{\frac{1}{d}} \exp\left(12\sqrt{d\ \log\ N\ \log\log\ N}\right) \ .$$

Proof. Let $S = [0,N]\times[0,N]$. The curve C has at most $\frac{1}{2}d(d-1)$ singular points, and at most $2d(d-1)$ points with slope ± 1. Hence $C \cap S$ is made up of at most $3d^2$ graphs of C^∞ functions with slope bounded by 1 with respect to one of the axes. The number of integral points is therefore at most

$$3d^2G(N) \le 3d^2N^{\frac{1}{d}} \exp\left(11\sqrt{d\ \log\ N\ \log\log\ N}\right) \ .\Box$$

If $d \ge 2$, the bound

$$O\left(\sqrt{N}\log\ N\right) \ ,$$

which is stronger than ours if $d = 2$, can be obtained using the large sieve in a similar way to that of Example 3 of Bombieri [1]. The idea of using the sieve in this connection has occurred to several authors, the earliest we could find being S.D. Cohen [2]. Those methods do not appear to give our stronger result for higher degree.

4. Integral Points on Smooth Curves

We now turn our attention to curves with many derivatives, and in particular to smooth curves. Initially we consider the homothetic dilations of a fixed curve, and later we make some uniform statements in terms of the number of zeros of derivatives of high order. According to the Main Lemma, if $f(x)$ has $\frac{1}{2}(d+1)(d+2)-1$ continuous derivatives, then the integral points on the graph of f reside on quite few algebraic curves of degree at most d. The number of these points can be estimated using the results of the previous section.

Let I be a closed subinterval of $[0,1]$.

Theorem 6. *Let $d \geq 2$ and suppose that $f(x) \in C^{D-1}(I)$ is a strictly convex function. Let Γ be the graph of f for $x \in I$. Then the number of integral points on $N\Gamma$ is at most*

$$d\left\{ \left(D\sqrt{\|f\|_{N,D-1}}N \right)^{\frac{8}{3(d+3)}} + 1 \right\} N^{\frac{1}{2}} \exp\left(12\sqrt{d \ \log \ N \ \log\log \ N} \right)$$

provided $N \geq \exp(d^6)$.

Proof. According to the Main Lemma, the integral points of $N\Gamma$ reside on at most

$$\left(D\sqrt{\|f\|_{N,D-1}}N \right)^{\frac{8}{3(d+3)}} + 1$$

algebraic curves of degree $\leq d$. Since Γ has at most 2 intersections with any line, we can assume that the irreducible components of these curves do not consist of lines, so that such a curve has at most

$$\frac{1}{2} d \cdot N^{\frac{1}{2}} \exp\left(12\sqrt{d \ \log \ N \ \log\log \ N} \right)$$

integral points in a square of side N. □

The estimate in this theorem can be made uniform in terms of the number of zeros of $f^{(D)}$ on I, assuming now that $f \in C^D(I)$. Before pursuing such a result, we note the following immediate consequence of Theorem 6.

Theorem 7. *Let $f(x)$ be a C^∞ strictly convex function on an interval I. Let $\varepsilon > 0$. Then there is a constant $c(f,\varepsilon)$ such that if Γ is the graph of $f(x)$ for $x \in I$, then*

$$|t\Gamma \cap \mathbb{Z}^2| \leq c(f,\varepsilon) t^{\frac{1}{2}+\varepsilon}$$

for all $t \geq 1$. Hence the same estimate holds for the dilations of a C^∞ oval.

To get a uniform result we will use a recurrence argument, as in the algebraic case. Controlling the number of zeros of $f^{(D)}$ gives us control on the number of solutions of $f^{(i)}(x) = c$ for $i \leq D-1$, and hence control on the number of subdivisions we must make. As usual I is a closed subinterval of $[0,N]$.

Theorem 8. *Suppose $d \geq 4$, $N \geq 1$, and let $f(x) \in C^D(I)$ be a strictly convex function with $|f'| \leq 1$. Suppose $f^{(D)}$ has at most m zeros. Let Γ be the graph of f. Then*

$$|\Gamma \cap \mathbb{Z}^2| \leq (m+1)c(d)N^{\frac{1}{2}+\frac{3}{d+3}} \ .$$

Proof. It suffices to prove the theorem in the case $m = 0$. In this case, an equation of the form

$$f^{(i)}(x) = 0, \qquad i \leq D-1, \qquad c \in \mathbb{R}$$

has at most $D - i$ distinct solutions interior to I. Let

$$G(N) = G(d, N)$$

be the maximum number of integral points on the graph of a C^D convex function $g(x)$ on an interval of length at most N, with $|g'(x)| \leq 1$, and such that $g^{(D)}$ has no zeros in the interior of the interval.

If $g(x)$ is such a function, with domain I, and $A > 0$, we can divide I into at most

$$1 + 2\sum_{i=1}^{D-1}(D-i) \leq D^2$$

subintervals I_ν, such that for each I_ν and each $\ell = 1, \cdots, D-1$, either (i) or (ii) holds:

(i) $$|g^{(\ell)}(x)| \leq \ell! A^{\ell/(D-1)} N^{1-\ell} \quad \text{all } x \in I_\nu$$

(ii) $$|g^{(\ell)}(x)| \geq \ell! A^{\ell/(D-1)} N^{1-\ell} \quad \text{all } \ x \in I_\nu \ .$$

Using $\delta = 6d + 20$ to estimate the points on algebraic curves (so that $\frac{2}{\delta-2} \leq \frac{1}{3(d+3)}$), we obtain the following recursive bound for $G(N)$

$$G(N) \leq D^2 \cdot \frac{1}{2} d \cdot (d^4\delta^6)^{d\delta} \cdot N^{\frac{1}{2}+\frac{1}{3(d+3)}} \cdot 2\left(D\sqrt{A}N\right)^{\frac{8}{3(d+3)}} + D^2 G\left(2A^{-\frac{1}{D-1}}N\right) \ .$$

The rest of the argument is the same as in the proof of Theorem 4. □

References

[1] Bombieri, E., *Le grand crible dans la théorie analytique des nombres.* Astérisque **18**, Soc. Math. France, Paris, 2^e éd. 1987/1974.

[2] Cohen, S.D., The distribution of Galois groups and Hilbert irreducibility theorem, *Proc. Lond. Math. Soc.* (3) **43** (1981), 227–250.

[3] Hilbert, D. and A. Hurwitz, Über die diophantischen Gleichungen vom Geschlecht Null, *Acta Mathematica* **14** (1890–1891), 217–224.
[4] Jarnik, V., Über die Gitterpunkte auf konvexen Curven, *Math. Z.* **24** (1926), 500–518.
[5] Lewis, D.J. and K. Mahler, Representation of integers by binary forms, *Acta Arith.* **6** (1961), 333–363.
[6] Posse, C., Sur le terme complémentaire de la formule de M. Tchebychef donnant l'expression approchée d'une intégrale définie par d'autres prises entre les mêmes limites, *Bull. Sci. Math.* (2) **7** (1883), 214–224.
[7] Sarnak, P., Torsion points on varieties and homology of Abelian covers, Manuscript, 1988.
[8] Schmidt, W.M., Integer Points on Curves and Surfaces, *Monatsh. Math.* **99** (1985), 45–72.
[9] Schwarz, H.A., Verallgemeinerung eines analytischen Fundamentalsatzes, *Annali di Mat.* (2) **10** (1880), 129–136. Also *Gesammelte Mathematische Abhandlungen*. Julius Springer, Berlin 1890, Bd. 2, 296–302.
[10] Swinnerton–Dyer, H.P.F., The Number of Lattice Points on a Convex Curve, *J. Number Theory* **6** (1974), 128–135.

Appendix

We give here a construction which disproves the conjecture of Schmidt in the strongest form proposed, namely, that there is an absolute constant c such that if Γ is an arc in a square of side $N \geq 1$ given by $y = f(x)$, where f'' exists and is weakly monotonic, and vanishes for at most one value of x, then

$$|\Gamma \cap \mathbb{Z}^2| \leq c\sqrt{N} \ .$$

Our construction will give

$$|\Gamma \cap \mathbb{Z}^2| \geq \frac{1}{20}\sqrt{N \ \log \ N}$$

for suitable smooth curves Γ having the requisite properties in boxes of side N, with $N \to \infty$. The constant $\frac{1}{20}$ is mentioned merely for convenience and it can be replaced by a larger one (e.g. 0.5) rather easily.

Initially, we construct a C^1 function $f_0(x)$, consisting of pieces of parabolas with increasing second derivatives whose graph Γ_0 is contained in a box of side N, and contains at least

$$\frac{1}{10}\sqrt{N \ \log \ N}$$

integer points. We then find a C^∞ function $f(x)$ coinciding with $f_0(x)$ on large pieces of the domain of $f(x)$, with $f'(x)$ non-decreasing, whose graph Γ contains at least half the integral points of Γ_0.

Let

$$a_1, \cdots, a_M$$

be a finite, non-increasing sequence of positive integers. Let $x_0 = 0$ and set

$$x_i = \sum_{j=1}^{i} a_j^2 \ , \qquad\qquad i = 1, \cdots, M,$$

$$y_i = \sum_{j=1}^{i} (2j-1) a_j^2 \ , \qquad\qquad i = 1, \cdots, M \ .$$

Now let Γ_0 be the graph of the function $y = f_0(x)$ where $f_0(x)$ is defined on the interval $[x_0, x_M]$ as follows:

$$f_0(x) = \left(\frac{x - x_{i-1}}{a_i} \right)^2 + 2(i-1)(x - x_{i-1}) + y_{i-1}$$

for $x \in [x_{i-1}, x_i]$, $i = 1, \cdots, M$. Since

$$\left(\frac{x_i - x_{i-1}}{a_i} \right)^2 + 2(i-1)(x_i - x_{i-1}) + y_{i-1} = (2i-1)a_i^2 + y_{i-1} = y_i \ ,$$

the definition is consistent at the endpoints of the subintervals $[x_{i-1}, x_i]$, and since

$$2\frac{x_i - x_{i-1}}{a_i^2} + 2(i-1) = 2i \ ,$$

the function f_0 is C^1 on $[x_0, x_M]$. Clearly f_0'' exists except at the points x_i for $i = 1, \cdots, M-1$, and since the sequence a_i is non-increasing, f_0'' is non-decreasing where it exists, and is clearly non-vanishing.

The graph Γ_0 is contained in a box of side

$$y_M = \sum_{i=1}^{M} (2i-1) a_i^2 \ ,$$

and contains at least

$$\sum_{i=1}^{M} a_i$$

integer points — a_i of them in each subinterval (x_{i-1}, x_i).

We now choose

$$a_i = \left[\frac{C}{i} \right]$$

for some large positive C. This gives at least

$$\sum_{i=1}^{M} \left[\frac{C}{i} \right] \geq C \sum_{i=1}^{M} \frac{1}{i} - M \geq C \log \ M - M$$

integer points on a curve in a box of side at most

$$2C^2 \sum_{i=1}^{M} \frac{1}{i} \leq 2C^2(\log\ M + 1)\ .$$

Now taking

$$C = \sqrt{N/\log\ N}\ , \qquad M = 2[N^{\frac{1}{5}}] + 1\ ,$$

we get, for N sufficiently large, at least

$$\frac{1}{10}\sqrt{N\ \log\ N}$$

points on a curve in a box of side at most N . The choice $M = 2[N^{\frac{1}{5}}] + 1$ ensures that the sequence a_i is strictly decreasing.

We now show that, by sacrificing at most half of the integer points, we can obtain a smooth modification Γ of Γ_0 with weakly monotonic second derivative everywhere. The graph G_0 of $g_0 = f_0'$ is a convex polygon, with vertices $(x_i, 2i)$, $i = 0, 1, \cdots, M$. Let $\varepsilon > 0$ be sufficiently small. We change G_0 into a C^∞ graph G of a function $g \in C^\infty([x_0, x_M])$ as follows. For every odd i let σ_i be the broken line consisting of the graph of g_0 over $[x_i, x_{i+1} + \varepsilon]$ and let us replace it with a smooth arc γ_i, making sure that

(i) the resulting curvilinear polygon G is smooth
(ii) there is no change in area in the undergraph when we replace σ_i by γ_i
(iii) γ_i has a continuously increasing tangent everywhere.

Thus γ_i initially stays below σ_i and then crosses it to join smoothly to G_0. By property (ii), we have

$$\int_0^x g(u)\mathrm{du} = \int_0^x g_0(u)\mathrm{du} = f_0(x)$$

for $x \in [x_{i+1} + \varepsilon, x_{i+2}]$, i odd, and $f(x) = \int_0^x g(u)\mathrm{du}$ is the required modification. Since $f(0) = 0$, $f(x_M) = y_M$ we see that the graph γ of f is contained in a box of side N and, for small ε, contains at least

$$\sum_{i\ \text{odd}} a_i$$

integral points. Since the a_i are decreasing, Γ contains at least half as many integral points as did Γ_0.

In this example, f'' is weakly monotonic but not strictly monotonic. However, if we interchange the role of x and y we obtain examples in which the third derivative f''' never vanishes.