ACTA ARITHMETICA
115.4 (2004)

On the square-free sieve

by

H. A. Helfgott (Montréal)

1. Introduction. A *square-free sieve* is a result that gives an upper bound for how often a square-free polynomial may adopt values that are not square-free. More generally, we may wish to control the behavior of a function depending on the largest square factor of $P(x_1, \ldots, x_n)$, where P is a square-free polynomial.

We may aim at obtaining an asymptotic expression

$$\text{main term} + O(\text{error term}), \tag{1.1}$$

where the main term will depend on the application; in general, the error term will depend only on the polynomial P in question, not on the particular quantity being estimated. We can split the error term further into one term that can be bounded for every given P, and a second term, say $\delta(P)$, which may be rather hard to estimate, and which is unknown for polynomials P of high enough degree.

Given this framework, the strongest results in the literature may be summarized as follows:

$\deg_{\text{irr}}(P)$	$\delta(P(x))$	$\delta(P(x,y))$
1	$\sqrt{N}$	1
2	$N^{2/3}$	N
3	$N/(\log N)^{1/2}$	$N^2/\log N$
4		$N^2/\log N$
5		$N^2/\log N$
6		$N^2/(\log N)^{1/2}$

Here $\deg_{\text{irr}}(P)$ denotes the degree of the largest irreducible factor of P. The second column gives $\delta(P)$ for polynomials $P \in \mathbb{Z}[x]$ of given $\deg_{\text{irr}}(P)$, whereas the third column refers to homogeneous polynomials $P \in \mathbb{Z}[x, y]$. The trivial estimates would be $\delta(P(x)) \leq N$ and $\delta(P(x,y)) \leq N^2$. See Section 6 for attributions.

2000 *Mathematics Subject Classification*: Primary 11N32; Secondary 11N36, 11G05.

Our task can be divided into two halves. The first one, undertaken in Section 3, consists in estimating all terms but $\delta(N)$. We do as much in full generality for any P over any number field. The second half regards bounding $\delta(N)$. We improve on all estimates known for $\deg P \geq 3$:

$\deg_{\text{irr}}(P)$	$\delta(P(x))$	$\delta(P(x,y))$
3	$N/(\log N)^{0.6829\ldots}$	$N^{3/2}/\log N$
4		$N^{4/3}(\log N)^A$
5		$N^{(5+\sqrt{113})/8+\varepsilon}$
6		$N/(\log N)^{0.7043\ldots}$

Some important applications, e.g., the computation of the distribution of root numbers in generic families of elliptic curves, yield an expression such as (1.1) with the main term equal to zero. Our improvements on the error term then become (substantial) improvements on the upper and lower bounds.

Most of our improvements hinge on a change from a local to a global perspective. Such previous work in the field as was purely sieve-based can be seen as a series of purely local estimates on the density of points on curves of non-zero genus. Our techniques involve a mixture of sieves, height functions and sphere packings.

The present paper is motivated in part by applications that demand us to construe square-free sieves in a broader sense than may have been customary before. We sketch the most general setting in which a square-free sieve is meaningful and applicable, and provide statements of intermediate generality and concreteness. In particular, we show how to use a square-free sieve to give explicit estimates on the average of certain infinite products arising from L-functions.

2. Notation. Let n be a non-zero integer. We write $\tau(n)$ for the number of positive divisors of n, $\omega(n)$ for the number of prime divisors of n, and $\text{rad}(n)$ for the product of the prime divisors of n. Given a prime p, we write $v_p(n)$ for the non-negative integer j such that $p^j \mid n$ and $p^{j+1} \nmid n$. For any $k \geq 2$, we write $\tau_k(n)$ for the number of k-tuples $(n_1, \ldots, n_k) \in (\mathbb{Z}^+)^k$ such that $n_1 \cdots n_k = |n|$. Thus $\tau_2(n) = \tau(n)$. We adopt the convention that $\tau_1(n) = 1$. We let

$$\text{sq}(n) = \prod_{p^2 \mid n} p^{v_p(n)-1}.$$

We call a rational integer n *square-full* if $p^2 \mid n$ for every prime p dividing n. Given any non-zero rational integer D, we say that n is (D)-*square-full* if $p^2 \mid n$ for every prime p that divides n but not D.

We denote by $\mathscr{O}_K$ the ring of integers of a global or local field K. We let I_K be the semigroup of non-zero ideals of $\mathscr{O}_K$. Given a non-zero ideal $\mathfrak{a} \in I_K$, we write $\tau_K(\mathfrak{a})$ for the number of ideals dividing $\mathfrak{a}$, $\omega_K(\mathfrak{a})$ for the number of prime ideals dividing $\mathfrak{a}$, and $\mathrm{rad}_K(\mathfrak{a})$ for the product of the prime ideals dividing $\mathfrak{a}$. Given a positive integer k, we write $\tau_{K,k}(\mathfrak{a})$ for the number of k-tuples $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ of ideals of $\mathscr{O}_K$ such that $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_k$. Thus $\tau_2(\mathfrak{a}) = \tau(\mathfrak{a})$. We define $\varrho(\mathfrak{a})$ to be the positive integer generating $\mathfrak{a} \cap \mathbb{Z}$.

When we say that a polynomial $f \in \mathscr{O}_K[x]$ or $f \in K[x]$ is *square-free*, we always mean that f is square-free as an element of $K[x]$. Thus, for example, we say that $f \in \mathbb{Z}[x]$ is *square-free* if there is no polynomial $g \in \mathbb{Z}[x]$ such that $\deg g \geq 1$ and $g^2 \mid f$.

Given an elliptic curve E over $\mathbb{Q}$, we write $E(\mathbb{Q})$ for the set of rational (that is, $\mathbb{Q}$-valued) points of E. We denote by $\mathrm{rank}(E)$ the algebraic rank of $E(\mathbb{Q})$.

We write $\#S$ for the cardinality of a finite set S. Given two sets $S_1 \subset S_2$, we denote $\{x \in S_2 : x \notin S_1\}$ by $S_2 - S_1$.

By a *lattice* we always mean an additive subgroup of $\mathbb{Z}^2$ of finite index. For $S \subset [-N, N]$ a convex set and L a lattice,

$$\#(S \cap L) = \frac{\mathrm{Area}(S)}{[\mathbb{Z}^2 : L]} + O(N),$$

where the implied constant is absolute.

A *sector* is a connected component of a set of the form $\mathbb{R}^2 - (T_1 \cup \cdots \cup T_n)$, where n is a non-negative integer and T_i is a line going through the origin. Every sector S is convex.

3. Sieving

3.1. *Averaging infinite products.* Take a function $u : \mathbb{Z} \to \mathbb{C}$ defined as a product

$$u(n) = \prod_p u_p(n)$$

of functions $u_p : \mathbb{Z}_p \to \mathbb{C}$, one for each prime. One may wish to write the average of $u(n)$ as a product of p-adic integrals:

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} u(n) = \prod_p \int_{\mathbb{Z}_p} u_p(x)\, dx. \tag{3.1}$$

Unfortunately, such an expression is not valid in general. Even if all the integrals are defined and of modulus at most 1, the infinite product may not converge, and the average on the left of (3.1) may not be defined; even if the product does converge and the average is defined, the two may not be equal. (Take, for example, $u_p(x) = 1$ for $x \in \mathbb{Z}$, $u_p(x) = 0$ for $x \in \mathbb{Z}_p - \mathbb{Z}$.)

We will establish that (3.1) is in fact true when three conditions hold. The first one will be a local condition ensuring that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} u_p(n) = \int_{\mathbb{Z}_p} u_p(x)\,dx,$$

among other things. The second condition states that $u_p(x) = 1$ when $p^2 \nmid P(x)$, where $P(x)$ is a fixed polynomial with integer coefficients. Thus we know that we are being asked to evaluate a convergent product such as $\prod_p (1 - a_p/p^2)$, rather than, say, the product $\prod_p (1 - 1/p)$. The third and last condition is that there be a non-trivial bound on the term $\delta(P(x))$ mentioned in the introduction.

We can make classical square-free sieves fit into the present framework by setting $u_p(x) = 0$ when $p^2 \mid F(x)$ (see Section 5). In other instances, the full generality of our treatment becomes necessary: see [He] for the example

$$u(n) = \prod_p u_p(n) = \prod_p \frac{W_p(\mathscr{E}(n))}{W_{0,p}(\mathscr{E}(n))}, \tag{3.2}$$

where $\mathscr{E}$ is a family of elliptic curves, $W_p(E)$ is the local root number of an elliptic curve E, and $W_{0,p}(E)$ is a first-order approximation to $W_p(E)$. It seems reasonable to expect the present method to be applicable to the estimation of other such ratios arising from Euler products.

Definition 1. A function $f : \mathbb{Z}_p \to \mathbb{C}$ is *openly measurable* if, for every $\varepsilon > 0$, there is a partition $\mathbb{Z}_p = U_0 \cup U_1 \cup \cdots \cup U_k$ and a tuple of complex numbers $(y_1, \ldots, y_k)$ such that

(1) $|f(x) - y_j| < \varepsilon$ for $x \in U_j$, $1 \le j \le k$,
(2) $\text{meas}(U_0) < \varepsilon$,
(3) all U_j are open.

Every function $f : \mathbb{Z}_p \to \mathbb{C}$ continuous outside a set of measure zero is openly measurable.

Proposition 3.1. *For every prime p, let $u_p : \mathbb{Z}_p \to \mathbb{C}$ be an openly measurable function with $|u_{\mathfrak{p}}(x)| \le 1$ for every $x \in \mathbb{Z}_p$. Assume that $u_p(x) = 1$ unless $p^2 \mid P(x)$, where $P \in \mathbb{Z}[x]$ is a polynomial satisfying*

$$\#\{1 \le x \le N : \exists p > N^{1/2},\ p^2 \mid P(x)\} = o(N).$$

Let $u(n) = \prod_p u_p(n)$. Then (3.1) *holds.*

Proof. Since we are not yet being asked to produce estimates for the speed of convergence, we may adopt a simple procedure specializing to the ones in [Hoo, Ch. IV] and [Gre]. Let ε_0 be given. By Appendix A, Lemma A.1,

$$\left|1 - \int_{\mathbb{Z}_p} u_p(x)\,dx\right| = O(p^{-2}),$$

where the implied constant depends only on P. Hence

$$\Big|\prod_p \int_{\mathbb{Z}_p} u_p(x)\,dx - \prod_{p\le\varepsilon_0^{-1}} \int_{\mathbb{Z}_p} u_p(x)\,dx\Big| = O(\varepsilon_0).$$

Let

$$u'(x) = \prod_{p\le\varepsilon_0^{-1}} u_p(x).$$

Since $u'(x) = u(x)$ unless $p^2 \mid P(x)$ for some $p > \varepsilon_0^{-1}$,

$$\begin{aligned}\Big|\sum_{n=1}^N u(n) - \sum_{n=1}^N u'(n)\Big| &\le 2\#\{1\le x\le N : \exists p > \varepsilon_0^{-1},\, p^2 \mid P(x)\}\\ &\le 2 \sum_{\varepsilon_0^{-1}<p\le N^{1/2}} \sum_{\substack{1\le x\le N\\ p^2\mid P(x)}} 1\\ &\quad + 2\#\{1\le x\le N : \exists p > N^{1/2},\, p^2 \mid P(x)\}.\end{aligned}$$

By Appendix A, Lemma A.2,

$$\sum_{\varepsilon_0^{-1}<p\le N^{1/2}} \sum_{\substack{1\le x\le N\\ p^2\mid P(x)}} 1 = O\Big(\sum_{\varepsilon_0^{-1}<p\le N^{1/2}} N/p^2\Big) = O(\varepsilon_0 N),$$

where the implied constant depends only on P. By the assumption in the statement,

$$\#\{1\le x\le N : \exists p > N^{1/2},\, p^2 \mid P(x)\} \le \varepsilon_0 N$$

for N greater than some constant C_{ε_0}. It now remains to compare

$$\frac{1}{N}\sum_{n=1}^N u'(n) \quad \text{and} \quad \prod_{p<\varepsilon_0^{-1}} \int_{\mathbb{Z}_p} u_p(x)\,dx.$$

For every p, we are given a tuple $(y_1,\ldots,y_{k_p})$ and a partition $\mathbb{Z}_p = U_{p,0}\cup U_{p,1}\cup\cdots\cup U_{p,k_p}$ satisfying the conditions in Definition 1 with $\varepsilon = \varepsilon_0^2$. We can assume that $U_{p,1}, U_{p,2},\ldots,U_{p,k_p}$ are connected and $|y_1|,\ldots,|y_{k_p}| \le 1$. We have

$$\begin{aligned}\sum_{n=1}^N u'(n) &= \sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \sum_{\substack{1\le n\le N\\ n\in\bigcap_p U_{p,j_p}\cap\mathbb{Z}}} u'(n)\\ &= \sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \sum_{\substack{1\le n\le N\\ n\in\bigcap_p U_{p,j_p}\cap\mathbb{Z}}} \Big(\prod_{p<\varepsilon_0^{-1}} y_{p,j_p} + O((1+\varepsilon_0^2)^{\varepsilon_0^{-1}} - 1)\Big)\end{aligned}$$

$$= \sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \sum_{\substack{1\leq n\leq N\\ n\in\bigcap_p U_{p,j_p}\cap\mathbb{Z}}} \prod_{p<\varepsilon_0^{-1}} y_{p,j_p} + O(\varepsilon_0 N)$$

$$= \sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \prod_{p<\varepsilon_0^{-1}} y_{p,j_p} \#\Big\{1\leq n\leq N : n\in\bigcap_p U_{p,j_p}\cap\mathbb{Z}\Big\} + O(\varepsilon_0 N),$$

whereas

$$\prod_{p<\varepsilon_0^{-1}} \int_{\mathbb{Z}_p} u_p(x)\,dx = \sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \prod_{p<\varepsilon_0^{-1}} \int_{U_{p,j_p}} u_p(x)\,dx$$
$$= \sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \prod_{p<\varepsilon_0^{-1}} \mathrm{meas}(U_{p,j_p})(y_{p,j_p}+O(\varepsilon)).$$

The absolute value of

$$\sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \prod_{p<\varepsilon_0^{-1}} \mathrm{meas}(U_{p,j_p})(y_p+O(\varepsilon)) - \sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \prod_{p<\varepsilon_0^{-1}} \mathrm{meas}(U_{p,j_p})y_p$$

is at most a constant times

$$\sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \Big(\prod_{p<\varepsilon_0^{-1}} \mathrm{meas}(U_{p,j_p})(1+\varepsilon) - \prod_{p<\varepsilon_0^{-1}} \mathrm{meas}(U_{p,j_p})\Big)$$
$$\ll \prod_{p<\varepsilon_0^{-1}} (1+\varepsilon) - 1 \ll \varepsilon_0.$$

It is left to bound the difference between

$$\frac{1}{N} \sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} y_{p,j_p} \#\Big\{1\leq n\leq N : n\in\bigcap_p U_{p,j_p}\cap\mathbb{Z}\Big\}$$

and

$$\sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \prod_{p<\varepsilon_0^{-1}} \mathrm{meas}(U_{p,j_p})y_{p,j_p}.$$

It is enough to estimate

$$\sum_{\vec{j}\in\prod_{p<\varepsilon_0^{-1}}[0,k_p]} \Big(\prod_{p<\varepsilon_0^{-1}} \mathrm{meas}(U_{p,j_p}) - \frac{1}{N}\#\Big\{1\leq n\leq N : n\in\bigcap_p U_{p,j_p}\cap\mathbb{Z}\Big\}\Big). \tag{3.3}$$

When all j_p are positive, $\bigcap_p U_{p,j_p}\cap\mathbb{Z}$ is an arithmetic progression. Hence

$$N\prod_j \mathrm{meas}(U_{p,j_p}) - \#\Big\{1\leq n\leq N : n\in\bigcap_p U_{p,j_p}\cap\mathbb{Z}\Big\} \leq 1.$$

When some j_p are zero, we can use inclusion-exclusion to obtain

$$\left|\#\left\{1 \le n \le N : n \in \bigcap_p U_{p,j_p} \cap \mathbb{Z}\right\} - N \prod_j \text{meas}(U_{p,j_p})\right| \le \prod_{\substack{p \\ j_p = 0}} k_p.$$

Hence the absolute value of (3.3) is at most

$$\frac{1}{N} \prod_{p<\varepsilon_0^{-1}} (2k_p).$$

If $N > \varepsilon_0^{-1} \prod_{p<\varepsilon_0^{-1}} (2k_p)$, then clearly $N^{-1} \prod_{p<\varepsilon_0^{-1}} (2k_p) = O(\varepsilon_0)$.

We can conclude that, for $N \ge \max(C_{\varepsilon_0}, \varepsilon_0^{-1} \prod_{p<\varepsilon_0^{-1}} (2k_p))$,

$$\left| \lim_{N\to\infty} \sum_{n=1}^{N} u(n) - \prod_p \int_{\mathbb{Z}_p} u_p(x)\, dx \right| = O(\varepsilon_0),$$

where the implied constant depends only on P. ∎

The question now is to make Proposition 3.1 explicit, or rather, how to do so well. We desire strong bounds on the speed of convergence.

3.2. *Riddles.* We will now see a near-optimal way to sieve out square factors below a certain size. Since the procedure is highly formal, we will state it in fairly general terms. It will be effortless to derive statements on number fields and higher power divisors.

We write $P(\mathscr{P})$ for the set of all subsets of a given set $\mathscr{P}$.

DEFINITION 2. A *soil* is a tuple $(\mathscr{P}, \mathscr{A}, r, f)$, where $\mathscr{P}$ is a set, $\mathscr{A}$ is a finite set, r is a function from $\mathscr{A}$ to $P(\mathscr{P})$, and f is a function from $\mathscr{A} \times P(\mathscr{P})$ to $\mathbb{C}$.

The purpose of a sieve is to estimate

$$\sum_{a\in\mathscr{A}} f(a, r(a)) \tag{3.4}$$

given data on

$$\sum_{\substack{a\in\mathscr{A} \\ r(a)\supset d_1}} f(a, d_2) \tag{3.5}$$

for $d_1, d_2 \in P(\mathscr{P})$. A traditional formulation would set $f(a,d) = 0$ for d non-empty and $f(a, \emptyset) = 1$ for every a. We shall work with $f(a,d)$ bounded for the sake of simplicity.

We need a way to order $\mathscr{P}$. We will take as given a function $h : P(\mathscr{P}) \to \mathbb{Z}^+$ such that

(h1) $h(d_1 \cup d_2) \le h(d_1)h(d_2)$ for all $d_1, d_2 \in P(\mathscr{P})$ disjoint,

(h2) $\{d \in P(\mathscr{P}) : h(d) \le n\}$ is finite for every $n \in \mathbb{Z}$.

We will also need an estimate for (3.5) in terms of $h(d)$. In our applications, we will be able to assume

$$\text{(A1)}\qquad \sum_{\substack{a\in\mathscr{A}\\ r(a)\supset d}} 1 \le C_0\,\frac{XC_1^{\#d}}{h(d)} + C_0C_2^{\#d} \text{ for } d\subset\mathscr{P},$$

$$\text{(A2)}\qquad \sum_{\substack{a\in\mathscr{A}\\ r(a)\supset d_1}} f(a,d_2) = X\,\frac{g(d_1,d_2)}{h(d_1)} + r_{d_1,d_2} \text{ for } d_2\subset d_1\subset\mathscr{P},\ h(d)\le M_0,$$

where X, C_0, C_1 and C_2 are constants given by the soil, g is some function with desirable properties, and r_{d_1,d_2} is small in average. We shall mention explicitly when and whether we assume (h1), (h2), (A1) and (A2) to hold; we will also state our precise conditions on g and r_d when we assume (A2). We will henceforth write S_d and A_{d_1,d_2} for the sums on the left of (A1) and (A2), respectively.

The sieve we are about to propose is of use when $\{h(d)\}$ is fairly sparse; hence the title of the subsection.

We write $\mu(S)$ for $(-1)^{\#S}$.

PROPOSITION 3.2. *Let* $(\mathscr{P},\mathscr{A},r,f)$ *be a soil with* f *bounded. Let* $h : P(\mathscr{P})\to\mathbb{Z}^+$ *satisfy* (h1) *and* (h2). *Then, for every positive integer* M,

$$\Bigl|\sum_{a\in\mathscr{A}} f(a,r(a)) - \sum_{\substack{d\subset\mathscr{P}\\ h(d)\le M}}\sum_{d'\subset d}\mu(d-d')A_{d,d'}\Bigr|$$

is at most

$$\Bigl(\sum_{\substack{d\subset\mathscr{P}\\ M<h(d)\le M^2}} (3^{\#d}+3)S_d + \sum_{\substack{p\in\mathscr{P}\\ h(\{p\})>M^2}} S_{\{p\}}\Bigr)\max_{a,d} f(a,d).$$

Proof. For every $d\subset P$, let $\pi(d)=\{x\in d : h(\{x\})\le M\}$. By Möbius inversion,

$$\sum_{\substack{d\subset r(a)\\ x\in d\Rightarrow h(\{x\})\le M}}\sum_{d'\subset d}\mu(d-d')f(a,d') = f(a,\pi(r(a)))$$

for every $a\in\mathscr{A}$. Hence

$$\sum_{a\in\mathscr{A}} f(a,r(a)) = \sum_{a\in\mathscr{A}}(f(a,r(a)) - f(a,\pi(r(a)))) + \sum_{a\in\mathscr{A}}\delta_a + \sum_{\substack{d\subset\mathscr{P}\\ h(d)\le M}}\sum_{d'\subset d}\mu(d-d')A_{d,d'},$$

where we write

$$(3.6)\quad \delta_a = \sum_{\substack{d\subset r(a)\\ x\in d\Rightarrow h(\{x\})\le M}} \sum_{d'\subset d} \mu(d-d')f(a,d') - \sum_{\substack{d\subset r(a)\\ h(d)\le M}} \sum_{d'\subset d} \mu(d-d')f(a,d').$$

Since $a=\pi(a)$ unless some $x\in a$ satisfies $h(\{x\})>M$, we know that

$$\sum_{a\in\mathscr{A}} (f(a,r(a))-f(a,\pi(r(a)))) \le 2\max_{a,d} f(a,d) \sum_{\substack{x\in\mathscr{P}\\ h(\{x\})>M}} S_{\{x\}}.$$

Now take $a\in\mathscr{A}$ such that $\delta_a\ne 0$. Then $h(\pi(r(a)))>M$. Let d be a subset of a with $h(d)\le M$. We would like to show that there is a subset s of $r(a)$ such that $d\subset s$ and $M<h(s)\le M^2$. Since $h(d)\le M$, all elements $x\in d$ obey $h(\{x\})\le M$, and thus $d\subset\pi(r(a))$. Let $x_1,\dots,x_k$ be the elements of $\pi(r(a))-d$. Let $s_0=d$. For $1\le i\le k$, let $s_i=d\cup\{x_1,\dots,x_i\}$. Then $h(s_0)\le M$, $h(s_k)=h(\pi(r(a)))>M$ and $h(s_{i+1})\le h(s_i)h(\{x_i\})\le h(s_i)M$ by (h1). Hence there is an $0\le i<k$ such that $M<h(s_i)\le M^2$. Since $d\subset s_i$ and $s_i\subset\pi(r(a))$, we can set $s=s_i$.

Now we bound the second sum in (3.6) trivially:

$$\Bigg|\sum_{\substack{d\subset r(a)\\ h(d)\le M}} \sum_{d'\subset d} \mu(d-d')f(a,d')\Bigg| \le \max_{a,d}|f(a,d)| \sum_{\substack{d\subset r(a)\\ h(d)\le M}} 2^{\#d}.$$

By the foregoing discussion,

$$\sum_{\substack{d\subset r(a)\\ h(d)\le M}} 2^{\#d} \le \sum_{\substack{s\subset r(a)\\ M<h(s)\le M^2}} \sum_{d\subset s} 2^{\#d} = \sum_{\substack{s\subset r(a)\\ M<h(s)\le M^2}} 3^{\#s}.$$

(We are still assuming $\delta_a\ne 0$.) Since

$$\Bigg|\sum_{\substack{d\subset r(a)\\ x\in d\Rightarrow h(\{x\})\le M}} \sum_{d'\subset d} \mu(d-d')f(a,d')\Bigg| = |f(a,\pi(r(a)))| \le \max_{a,d} f(a,d),$$

and since (again by $\delta_a\ne 0$) we have

$$\sum_{\substack{s\subset r(a)\\ M<h(s)\le M^2}} 1 \ge 1,$$

we can conclude that

$$\sum_{a\in\mathscr{A}} \delta_a \le \max_{a,d}|f(a,d)| \sum_{a\in\mathscr{A}} \sum_{\substack{s\subset r(a)\\ M<h(s)\le M^2}} (3^{\#s}+1).$$

Clearly

$$\sum_{a\in\mathscr{A}} \sum_{\substack{s\subset r(a)\\ M<h(s)\leq M^2}} (3^{\#s}+1) \leq \sum_{\substack{d\subset\mathscr{P}\\ M<h(d)\leq M^2}} (3^{\#d}+1)S_d.$$

The statement follows. ■

COROLLARY 3.3. *Let* $(\mathscr{P},\mathscr{A},r,f)$ *be a soil with* $\max_{a,d} f(a,d) \leq C_3$. *Assume* (A1) *and* (A2) *with* $\max_{d_1,d_2} g(d_1,d_2) \leq C_4$. *Let* h *be multiplicative and satisfy* (h2). *Then, for every* $M \leq M_0$,

$$\Big|\sum_{a\in\mathscr{A}} f(a,r(a)) - X\sum_{d\subset\mathscr{P}}\sum_{d'\subset d}\mu(d-d')\,\frac{g(d,d')}{h(d)}\Big|$$

is at most

$$X\sum_{\substack{d\subset\mathscr{P}\\ h(d)>M}} \frac{1}{h(d)}\,(C_4 2^{\#d} + C_3C_0C_1^{\#d}(3^{\#d}+3)) \tag{3.7}$$
$$+ C_3 \sum_{\substack{d\subset\mathscr{P}\\ M<h(d)\leq M^2}} C_0C_2^{\#d}(3^{\#d}+3) + \sum_{\substack{d\subset\mathscr{P}\\ h(d)\leq M}}\sum_{d'\subset d}|r_{d,d'}| + C_3\sum_{\substack{p\in\mathscr{P}\\ h(\{p\})>M^2}} S_{\{p\}}.$$

Proof. Apply Proposition 3.2. By (A1),

$$\sum_{\substack{d\subset\mathscr{P}\\ M<h(d)\leq M^2}} (3^{\#d}+3)S_d \leq X\sum_{\substack{d\subset\mathscr{P}\\ M<h(d)\leq M^2}} C_0\,\frac{C_1^{\#d}}{h(d)}\,(3^{\#d}+3) + \sum_{\substack{d\subset\mathscr{P}\\ M<h(d)\leq M^2}} C_0C_2^{\#d}(3^{\#d}+3).$$

By (A2),

$$\sum_{\substack{d\subset\mathscr{P}\\ h(d)\leq M}}\sum_{d'\subset d}\mu(d-d')A_{d,d'} = X\sum_{\substack{d\subset\mathscr{P}\\ h(d)\leq M}}\sum_{d'\subset d}\mu(d-d')\,\frac{g(d,d')}{h(d)} + \sum_{\substack{d\subset\mathscr{P}\\ h(d)\leq M}}\sum_{d'\subset d}\mu(d-d')r_{d,d'}.$$

Finally,

$$\Big|\sum_{\substack{d\subset\mathscr{P}\\ h(d)>M}}\sum_{d'\subset d}\mu(d-d')\,\frac{g(d,d')}{h(d)}\Big| \leq \sum_{\substack{d\subset P\\ h(d)>M}} \frac{C_4 2^{\#d}}{h(d)}. \ ■$$

PROPOSITION 3.4. *Let* K *be a number field. Let* $Q \in \mathscr{O}_K[x]$ *be a polynomial. Let* m *be a positive integer. Then the number of positive integers*

$x \le N$ for which $Q(x)$ is free of mth powers equals

$$N \prod_p \left(1 - \frac{\ell(p^m)}{p^m}\right) + O(N^{2/(m+1)}(\log N)^C) \\ + O(\#\{1 \le x \le N : \exists p > N^{2/(m+1)},\, p^m \mid Q(x)\}),$$

where

$$\ell(p^m) = \#\{x \in \mathbb{Z}/p^m : \mathfrak{p}^m \mid Q(x) \text{ for some } \mathfrak{p} \in I_K \text{ above } p\}.$$

The implied constant and C depend only on K and Q.

Proof. We define a soil $(\mathscr{P}, \mathscr{A}, r, f)$ by

$$\mathscr{P} = \{\mathfrak{p} \in I_K : \mathfrak{p} \text{ prime}\}, \qquad \mathscr{A} = \{1, \ldots, N\},$$
$$r(a) = \{\mathfrak{p} \in \mathscr{P} : \mathfrak{p}^m \mid Q(a)\}, \quad f(a,d) = \begin{cases} 1 & \text{if } d = \emptyset, \\ 0 & \text{otherwise.} \end{cases}$$

Let $h(d)$ be the positive integer generating the ideal $(\prod_{\mathfrak{p} \in d} \mathfrak{p}^m) \cap \mathbb{Z}$. Properties (h1) and (h2) are clear. Lemma A.2 gives us properties (A1) and (A2) with

$$X = N, \quad g(d_1, d_2) = 0 \quad \text{if } d_2 \text{ non-empty},$$
$$g(d, \emptyset) = \#\{x \in \mathbb{Z}/h(d) : \mathfrak{p}^m \mid Q(x)\ \forall \mathfrak{p} \in d\},$$
$$|r_{d,\emptyset}| \le |\operatorname{Disc} Q|^3 (\deg Q)^{\#d}, \quad |r_{d_1,d_2}| = 0 \quad \text{if } d_2 \text{ non-empty},$$
$$C_0 \ll |\operatorname{Disc} Q|^3, \quad C_1, C_2 \ll \deg Q, \quad M_0 = N.$$

By Corollary 3.3,

$$\sum_{a \in \mathscr{A}} f(a, r(a)) - N \sum_{d \subset \mathscr{P}} \sum_{d' \subset d} \mu(d - d') \frac{g(d,d')}{h(d)}$$

is at most

$$N \sum_{\substack{d \subset \mathscr{P} \\ h(d) > M}} \frac{1}{h(d)} (2^{\#d} + C_0 C_1^{\#d}(3^{\#d} + 3)) + \sum_{\substack{d \subset \mathscr{P} \\ M < h(d) \le M^2}} C_0 C_2^{\#d}(3^{\#d} + 3) \\ + \sum_{\substack{d \subset \mathscr{P} \\ h(d) \le M}} |\operatorname{Disc} Q|^3 (\deg Q)^{\#d} + \sum_{\substack{p \in \mathscr{P} \\ h(\{p\}) > M^2}} S_{\{p\}}.$$

Given a positive integer n, there are at most $2^{(\deg K/\mathbb{Q})\omega(n)}$ elements d of $\mathscr{P}$ such that $h(d) = m$. Moreover, for every prime p not ramified in $K/\mathbb{Q}$, $p \mid h(d)$ implies $p^m \mid h(d)$. Hence

$$N \sum_{\substack{d \subset \mathscr{P} \\ h(d) > M}} \frac{c^{\#d}}{h(d)} \ll N \sum_{n > M^{1/m}} \frac{(2^{\deg K/\mathbb{Q}} c)^{\omega(n)}}{n^m} \ll N \frac{(\log M)^{2^{2^{\deg K/\mathbb{Q}} c} - 1}}{N^{(m-1)/m}},$$

$$\sum_{\substack{d\subset\mathscr{P}\\ M<h(d)\le M^2}} c^{\#d} \ll M^{2/m}(\log M)^{2^c-1}, \qquad \sum_{\substack{d\subset\mathscr{P}\\ h(d)\le M}} c^{\#d} \ll M^{1/m}(\log M)^{2^c-1}.$$

We choose $M = N^{m/(m+1)}$, since then $N/M^{(m-1)/m} = M^{2/m}$.

It remains to show that

$$\sum_{d\subset\mathscr{P}}\sum_{d'\subset d}\mu(d-d')\,\frac{g(d,d')}{h(d)} = \prod_p\left(1-\frac{\ell(p^m)}{p^m}\right).$$

By (3.2),

$$\begin{aligned}\sum_{d\subset\mathscr{P}}\sum_{d'\subset d}\mu(d-d')\,\frac{g(d,d')}{h(d)} &= \sum_{d\subset\mathscr{P}}\mu(d)\,\frac{g(d,0)}{h(d)}\\ &= \prod_{p\text{ prime}}\sum_{\substack{d\subset\mathscr{P}\\ h(d)=p}}\mu(d)\,\frac{g(d,0)}{h(d)} = \prod_{p\text{ prime}}\left(1-\frac{\ell(p^m)}{p^m}\right)\end{aligned}$$

and so we are done. ■

While the following result could be stated in the same generality as Proposition 3.4, we restrict ourselves to the rationals and to square divisors in order to avoid inessential complications.

PROPOSITION 3.5. *Let $Q\in\mathbb{Z}[x,y]$ be a homogeneous polynomial. Then the number of pairs of positive integers $x,y\le N$ for which $Q(x,y)$ is free of mth powers equals*

$$\begin{aligned}N^2\prod_p\left(1-\frac{\ell(p^2)}{p^4}\right) &+ O(N^{3/2}(\log N)^C)\\ &+ O(\#\{1\le x,y\le N : \exists p>N,\ p^2\,|\,Q(x,y)\}),\end{aligned}$$

where $\ell(p^2) = \#\{x,y\in\mathbb{Z}/p^2 : p^2\,|\,Q(x,y)\}$. The implied constant and C depend only on Q.

Proof. We define a soil $(\mathscr{P},\mathscr{A},r,f)$ by

$$\mathscr{P} = \{p\in\mathbb{Z}^+ : p \text{ prime}\}, \qquad \mathscr{A} = \{1\le x,y\le N : \gcd(x,y)=1\},$$
$$r(a) = \{p\in\mathscr{P} : p^2\,|\,Q(a)\}, \qquad f(a,d) = \begin{cases}1 & \text{if } d\ne\emptyset,\\ 0 & \text{otherwise.}\end{cases}$$

Let $h(d) = \prod_{p\in d}p^2$. Properties (h1), (h2), (A1) and (A2) hold by Lemmas A.3–A.5 with

$$X = N^2 \prod_p \left(1 - \frac{1}{p^2}\right), \qquad g(d_1, d_2) = 0 \quad \text{if } d_2 \text{ non-empty},$$

$$g(d, \emptyset) = \frac{\#\{x, y \in \mathbb{Z}/h(d) : p^2 \mid Q(x,y) \wedge (p \nmid x \vee p \nmid y)\ \forall p \in d\}}{\prod_{p \in d}(p^2 - 1)},$$

$$|r_{d,\emptyset}| \le |\operatorname{Disc} Q|^3 (2 \deg Q)^{\# d} N \log N, \qquad r_{d_1,d_2} = 0 \quad \text{if } d_2 \text{ non-empty},$$

$$C_0 \ll |\operatorname{Disc} Q|^3, \qquad C_1, C_2 = 2 \deg Q, \qquad M_0 = N.$$

By Corollary 3.3,

$$\sum_{a \in \mathscr{A}} f(a, r(a)) - X \sum_{d \in \mathscr{P}} \sum_{d' \subset d} \mu(d - d') g(d)$$

is at most

$$N^2 \prod_p \left(1 - \frac{1}{p^2}\right) \sum_{n > M^{1/2}} \frac{1}{n^2} \left(2^{\omega(n)} + C_0 C_1^{\omega(n)} (3^{\omega(n)} + 3)\right) + \sum_{\substack{p \text{ prime} \\ p > M}} S_{\{p\}}$$

$$+ \sum_{M^{1/2} < n \le M} C_0 C_2^{\omega(n)} (3^{\omega(n)} + 3) + \sum_{n \le M^{1/2}} |\operatorname{Disc} Q|^3 (2 \deg Q)^{\omega(n)} N \log N,$$

which in turn is at most

$$N^2 \frac{(\log M)^C}{M^{1/2}} + M (\log M)^C + M^{1/2} N \log N + \sum_{\substack{p \text{ prime} \\ p > M}} S_{\{p\}}$$

for some C given by C_0, C_1, C_2.

We set $M = N$. Now

$$\sum_{d \subset \mathscr{P}} \sum_{d' \subset d} \mu(d - d') \frac{g(d, d')}{h(d)} = \sum_{d \subset \mathscr{P}} \mu(d) \frac{g(d, \emptyset)}{h(d)} = \prod_p \left(1 - \frac{\ell'(p^2)}{p^4}\right),$$

where

$$\ell'(p^2) = \#\{x, y \in \mathbb{Z}/p^2 : p^2 \mid Q(x,y) \wedge (p \nmid x \vee p \nmid y)\}/(p^2 - 1).$$

Clearly $\ell'(p^2)(p^2 - 1) = \ell(p^2) - p^2$. Hence

$$\prod_p \left(1 - \frac{\ell'(p^2)}{p^2}\right) = \prod_p \left(1 - \frac{\ell(p^2) - p^2}{p^2(p^2 - 1)}\right)$$

$$= \prod_p \frac{p^4 - \ell(p^2)}{p^2(p^2 - 1)} = \prod_p \left(1 - \frac{\ell(p^2)}{p^4}\right) \Big/ \prod_p \left(1 - \frac{1}{p^2}\right).$$

The statement follows. ∎

3.3. *Sampling and averaging.* A slight layer of abstraction is now called for. Let J_0 be an index set. Let V_j, $j \in J_0$, be measure spaces with positive measures μ_j, $j \in J_0$. Consider a countable set Z together with injections $\iota_j : Z \to V_j$ for every $j \in J_0$, and a finite subset $Z_j \subset Z$ for every $n \in \mathbb{Z}^+$.

Let $\mathscr{M}_j$ be a collection of measurable subsets of V_j, each of them of finite measure. Let $\upsilon : \mathbb{Z}^+ \to \mathbb{R}_0^+$ be a function with $\lim_{n\to\infty} \upsilon(n) = 0$. Assume that

$$\left|\frac{1}{\#Z_n} \sum_{x\in Z_n \cap \bigcap_{j\in J} \iota_j^{-1}(M_j)} 1 - \prod_{j\in J} \mu_j(M_j)\right| \le \upsilon(n) \tag{3.8}$$

for every finite subset $J \subset J_0$ and every tuple $\{M_j\}_{j\in J}$, $M_j \in \mathscr{M}_j$.

We may call Z the *sample frame*, and $\mathscr{M}_j$, $j \in J_0$, the *sampling spaces.* A tuple $(J_0, \{V_j\}, Z, \{\iota_j\}, \{Z_n\}, \upsilon, \{\mathscr{M}_j\})$ satisfying the conditions above, including (3.8), will be called a *sampling datum.* Given a measure σ_j on V_j and a function $s_j : Z \to \mathbb{C}$ for every $j \in J$, we say $(\{s_j\}, \{\sigma_j\})$ is a *distribution pair* if $\max(|s_j(x)|) \le 1$, $\max|\sigma_j/\mu_j| \le 1$, and

$$\left|\frac{1}{\#Z_n} \sum_{x\in Z_n \cap \bigcap_{j\in J} \iota_j^{-1}(M_j)} s(x) - \prod_{j\in J} \sigma_j(M_j)\right| \le \upsilon_0(n) \prod_{j\in J} \mu_j(M_j) + \upsilon_1(n)$$

for every finite subset $J \subset J_0$ and every tuple $\{M_j\}_{j\in J}$, $M_j \in \mathscr{M}_j$, where $\upsilon_0(n), \upsilon_1(n) : \mathbb{Z}^+ \to \mathbb{R}_0^+$ are functions with $\lim_{n\to\infty} \upsilon_0(n) = \lim_{n\to\infty} \upsilon_1(n) = 0$ and we write $s(x)$ for $\prod_{j\in J} s_j(x)$.

Given a positive integer c, we define $\mathscr{M}_{c,j}$ to be the collection of all sets of the form

$$(M_1 \cup \cdots \cup M_{n_1}) - (M_1' \cup \cdots \cup M_{n_2}'),$$

where $M_1, \ldots, M_{n_1} \in \mathscr{M}_j$ and $M_1', \ldots, M_{n_2}' \in \mathscr{M}_j$ and $n_1 + n_2 \le c$. It should be clear that (3.8) and the inequality following it hold for $M_j \in \mathscr{M}_{c,j}$ if the terms on the right are multiplied by $c^{\#J}$.

Let j be an element of J_0. Let $M_j \in \mathscr{M}_j$. Let $m : \mathbb{R}^+ \to \mathbb{R}^+$ be a decreasing function with $\int_0^\infty m(x)\,dx < \infty$. Let c be a positive integer. A function $f : M_j \to \mathbb{C}$ is (c,m)-*approximable* if there is a partition $M_j = M_{j,0} \cup M_{j,1} \cup \cdots$ and a sequence $\{y_i\}_{i\ge 1}$ of complex numbers such that

(1) $M_{j,i} \in \mathscr{M}_{j,i}$ for $i \ge 1$,
(2) $f(x) = y_i$ for $x \in U_i$, $i \ge 1$,
(3) $\mu_j(M_{j,0}) = 0$,
(4) $\mu_j(M_{j,i}) \le m(i)$ for every $i \ge 1$.

LEMMA 3.6. *Let $(J_0, \{V_j\}, Z, \{\iota_j\}, \{Z_n\}, \upsilon, \{\mathscr{M}_j\})$ be a sampling datum, (s_j, σ_j) a distribution pair. Let J be a finite subset of J_0. For every $j \in J$, choose $M_j \in \mathscr{M}_j$ and let $u_j : M_j \to \mathbb{C}$ be a (c, m_j)-approximable function with $\max_x |u_j(x)| \le 1$. Write $u(x) = \prod_{j\in J} u_j(x)$, $s(x) = \prod_{j\in J} s_j(x)$, $c_0 = c^{\#J}$. Then, for every subset S of $(\mathbb{Z}^+)^J$,*

$$\left|\frac{1}{\#Z_n} \sum_{x\in Z_n \cap \bigcap_{j\in J} \iota_j^{-1}(M_j)} s(x)u(x) - \prod_{j\in J} \int_{M_j} u_j(x)\,d\sigma_j\right|$$

is at most

$$\sum_{(t_j)\in(\mathbb{Z}^+)^J-S}\prod_{j\in J} m_j(t_j) + c_0\upsilon_0(n)\prod_{j\in J}\mu_j(M_j) + (\#S)c_0\upsilon_1(n) + (\#S+1)c_0\upsilon(n). \tag{3.9}$$

Proof. Since $|\sigma_j/\mu_j|\le 1$, $|u_j|\le 1$ and u_j is m_j-approximable,

$$\begin{aligned}\Big|\prod_{j\in J}\int_{M_j} u_j(x)\,d\sigma_j - \sum_{(t_j)\in S}\prod_{j\in J}\int_{M_{j,t_j}} u_j(x)\,d\sigma_j\Big| \\ = \Big|\sum_{(t_j)\in(\mathbb{Z}^+)^J-S}\prod_{j\in J}\int_{M_{j,t_j}} u_j(x)\,d\sigma_j\Big| \le \sum_{(t_j)\in(\mathbb{Z}^+)^J-S}\prod_{j\in J} m_j(t_j),\end{aligned}$$

whereas $\prod_{j\in J}\int_{M_{j,t_j}} u_j(x)\,d\sigma_j = \prod_{j\in J} y_j\sigma_j(M_{j,t_j})$. Now

$$\Big|\prod\sigma_j(M_{j,t_j}) - \frac{1}{\#Z_n}\sum_{x\in Z_n\cap\bigcap_{j\in J}\iota_j^{-1}(M_{j,t_j})} s(x)\Big|$$

is at most

$$c_0\upsilon_0(n)\prod_{j\in J}\mu_j(M_{j,s_j}) + c_0\upsilon_1(n).$$

Clearly

$$\begin{aligned}\sum_{(t_j)\in S} c_0\upsilon_0(n)\prod_{j\in J}\mu_j(M_{j,t_j}) &= c_0\upsilon_0(n)\sum_{(t_j)\in(\mathbb{Z}^+)^J}\prod_{j\in J}\mu_j(M_{j,t_j}) \\ &= c_0\upsilon_0(n)\prod_{j\in J}\mu_j(M_j).\end{aligned}$$

By (3.8),

$$\begin{aligned}\Big|\sum_{(t_j)\notin S}\frac{1}{\#Z_n}\sum_{x\in Z_n\cap\bigcap_{j\in J}\iota_j^{-1}(M_{j,t_j})} s(x)\Big| &\le \sum_{(t_j)\notin S}\frac{1}{\#Z_n}\sum_{x\in Z_n\cap\bigcap_{j\in J}\iota_j^{-1}(M_{j,t_j})} 1 \\ &= \frac{\#(Z_n\cap\bigcap_{j\in J}\iota_j^{-1}(M_j))}{\#Z_n} - \sum_{(t_j)\in S}\frac{1}{\#Z_n}\sum_{x\in Z_n\cap\bigcap_{j\in J}\iota_j^{-1}(M_{j,t_j})} 1 \\ &= \prod_{j\in J}\mu_j(M_j) - \sum_{(t_j)\in S}\prod_{j\in J}\mu_j(M_{j,t_j}) + O(c_0(\#S+1)\upsilon(n)) \\ &= \sum_{(t_j)\in(\mathbb{Z}^+)^J-S}\prod_{j\in J}\mu_j(M_{j,t_j}) + O(c_0(\#S+1)\upsilon(n)).\end{aligned}$$

Both implied constants have absolute value at most 1. The statement follows. ∎

It is time to produce some examples of sampling data.

Example 1. Let J_0 be the set of rational primes. Let $V_p = \mathbb{Z}_p$, $Z = \mathbb{Z}$, $Z_n = \{1, \dots, n\}$, $\iota_p : \mathbb{Z} \to \mathbb{Z}_p$ the natural injection, $\mathscr{M}_p$ the set of additive subgroups of $\mathbb{Z}_p$ of finite index, $v(n) = 1/n$. Then $(J_0, \{V_p\}, Z, \{\iota_p\}, \{Z_n\}, v, \{\mathscr{M}_p\})$ is a sampling datum.

Example 2. Let J_0 be the set of rational primes. Let $S \subset \mathbb{R}^2$ be a sector. Let $V_p = \mathbb{Z}_p^2$, $Z = \mathbb{Z}^2 \cap S$, $Z_n = \{-n \le x, y \le n\} \cap S$, $\iota_p : \mathbb{Z} \to \mathbb{Z}_p$ the natural injection, $v(n) = O(1/n)$, $\mathscr{M}_p$ the set of all additive subgroups of $\mathbb{Z}_p^2$ of finite index. Then $(J_0, \{V_p\}, Z, \{\iota_p\}, \{Z_n\}, v, \{\mathscr{M}_p\})$ is a sampling datum. The implied constant in $v(n) = O(1/n)$ is absolute.

Example 3. Let J_0 be the set of rational primes. Let $S \subset \mathbb{R}^2$ be a sector. Let $V_p = \mathbb{Z}_p^2 - p\mathbb{Z}_p^2$, $Z = \{x, y \in \mathbb{Z} : \gcd(x, y) = 1\} \cap S$, $Z_n = \{-n \le x, y \le n : \gcd(x, y) = 1\} \cap S$, $v(n) = O(\log n/n)$, $\mathscr{M}_p$ the collection of sets of the form $L \cap Z$, where by L we mean an additive subgroup of $\mathbb{Z}_p^2$ of finite index. By Lemma A.4, $(J_0, \{V_p\}, Z, \{\iota_p\}, \{Z_n\}, v, \{\mathscr{M}_p\})$ is a sampling datum. The implied constant in $v(n) = O(\log n/n)$ is absolute.

The datum in Example 3 is more natural than that in Example 2 when the pairs $(x, y) \in \mathbb{Z}^2$ are meant to represent rational numbers x/y.

3.4. *Averages.* We can now give explicit analogues of Proposition 3.1. Our conditions on the behavior of u_p are fairly strict; somewhat laxer conditions can be adopted with a consequent degradation in the quality of the bounds.

Proposition 3.7. *For every prime p, let $u_p : \mathbb{Z}_p \to \mathbb{C}$ be a $(c_0, c_1 p^{-c_2 j})$-approximable function, where c_0 is a positive integer and c_1, c_2 are positive real numbers. Assume that $|u_p(x)| \le 1$ for every $x \in \mathbb{Z}_p$. Assume, furthermore, that $u_p(x) = 1$ unless $p^2 \mid P(x)$, where $P \in \mathbb{Z}[x]$ is a fixed square-free polynomial. Then*

$$\frac{1}{N} \sum_{n=1}^{N} \prod_p u_p(n) = \prod_p \int_{\mathbb{Z}_p} u_p(x)\, dx + O((\log N) N^{-1/3}) + \frac{1}{N} O(\#\{1 \le x \le N : \exists p > N^{2/3},\ p^2 \mid P(x)\}),$$

where the implied constant depends only on P, c_0, c_1 and c_2.

Proof. We define a soil $(\mathscr{P}, \mathscr{A}, r, f)$ by

$$\mathscr{P} = \{p \in \mathbb{Z}^+ : p \text{ prime}\}, \qquad \mathscr{A} = \{1, \dots, N\},$$
$$r(a) = \{p \in \mathscr{P} : p^2 \mid P(a)\}, \qquad f(a, d) = \textstyle\prod_{p \in d} u_p(a).$$

Let $h(d) = \prod_{p \in d} p^2$. Properties (h1) and (h2) are clear. Lemma A.2 gives us property (A1) with

$$X = N, \quad C_0 \ll |\mathrm{Disc}\, P|^3, \quad C_1, C_2 \ll \deg P.$$

Choose the sampling datum in Example 1 with $n = N$. By Lemma 3.6, property (A2) then holds with

$$g(d_1, d_2) = h(d_1) \prod_{p\in d_2} \int_{D_p} u_p(x)\, d\mu_p \prod_{p\in d_1 - d_2} \int_{D_p} d\mu_p$$
$$= h(d_1) \prod_{p\in d_1 - d_2} \mu(D_p) \prod_{p\in d_2} \int_{D_p} u_p(x)\, d\mu_p,$$

where $D_p = \{x \in \mathbb{Z}_p : p^2 \mid P(x)\}$,

$$r_{d_1,d_2} \le N \sum_{(t_p)\in(\mathbb{Z}^+)^{d_1} - S} \prod_{p\in d_1} m_p(t_p) + c_0^{\#d_1} \sum_{(t_p)\in S} 1 + c_0^{\#d_1}(\#S + 1)$$
$$= N \sum_{(t_p)\in(\mathbb{Z}^+)^{d_1} - S} \prod_{p\in d_1} m_p(t_p) + c_0^{\#d_1}(2\#S + 1)$$

for every $S \in (\mathbb{Z}^+)^{d_1}$ and $m_p(j) = c_1 p^{-c_2 j}$. (We can set M_0 arbitrarily large.) Choose

$$S = \bigtimes_{p\in d_1} \left\{ n \in \mathbb{Z} : 1 \le n \le \frac{c_2 \log N}{\log p} \right\}. \tag{3.10}$$

Then

$$\sum_{(s_p)\in(\mathbb{Z}^+)^{d_1} - S} \prod_{p\in d_1} m_p(s_p) \le \sum_{p\in d_1} \sum_{j > c_2 \log N/\log p} m_p(j)$$
$$\le \sum_{p\in d_1} \frac{c_1}{1 - p^{-c_2}} \exp\left(-\frac{c_2 \log N}{\log p} \frac{\log p}{c_2} \right)$$
$$= \frac{c_1}{1 - 2^{-c_2}} \#d_1/N,$$

and so

$$r_{d_1,d_2} \le 2c_0^{\#d_1} \prod_{p\in d_1} \left(\frac{c_2 \log N}{\log p} \right) + \frac{c_1}{1 - 2^{-c_2}} \#d_1 + c_0^{\#d_1}.$$

We can now apply Corollary 3.3. We deduce that the absolute value of the difference

$$\sum_{a\in\mathscr{A}} f(a, r(a)) - N \sum_{d\in\mathscr{P}} \sum_{d'\subset d} \mu(d - d') \frac{g(d, d')}{h(d)}$$
$$= \sum_{n=1}^{N} \prod_p u_p(n) - N \sum_{d\,\text{square-free}} \sum_{d'|d} \mu(d/d') \prod_{p|d/d'} \mu_p(D_p) \prod_{p|d'} \int_{D_p} u_p(x)\, d\mu_p$$
$$= \sum_{n=1}^{N} \prod_p u_p(n) - N \prod_p \int_{\mathbb{Z}_p} u_p(x)\, d\mu_p$$

is at most (3.7) with $C_3 = C_4 = 1$ and M arbitrary. The first term of (3.7) is $O((\log M)^c M^{-1/2} N)$, where c and the implied constant depend only on C_0, C_1 and C_2. The second term is $O(M(\log M)^c)$. By Lemma B.2, the third term is no greater than

$$\sum_{\substack{1\le d\le M^{1/2}\\ d\,\text{square-free}}} \sum_{d'|d} \left(2c_0^{\omega(d)} \prod_{p|d} \frac{c_2 \log N}{\log p} + \frac{c_1}{1-p^{-c_2}}\,\omega(d) + c_0^{\omega(d)}\right) \ll M^{1/2+\varepsilon}.$$

Set $M = N^{2/3}$. The result follows. ■

Proposition 3.8. *For every p, let $u_p : \mathbb{Z}_p^2 - p\mathbb{Z}_p^2 \to \mathbb{C}$ be a $(c_0, c_1 p^{-c_2})$-approximable function, where c_0 is a positive integer and c_1, c_2 are positive real numbers. Assume that $|u_p(x,y)| \le 1$ for all $(x,y) \in \mathbb{Z}_p^2 - p\mathbb{Z}_p^2$. Assume, furthermore, that $u_p(x,y) = 1$ for all $(x,y) \in \mathbb{Z}_p^2 - p\mathbb{Z}_p^2$ such that $p^2 \nmid P(x)$, where $P \in \mathbb{Z}[x,y]$ is a fixed square-free homogeneous polynomial.*

Let $S \subset \mathbb{R}^2$ be a sector. Then

$$\sum_{\substack{-N\le x,y\le N\\ (x,y)\in S\\ \gcd(x,y)=1}} \prod_p u_p(x,y)$$

equals

$$(\#(S\cap[-N,N]^2)) \prod_p \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} u_p(x,y)\,dx\,dy + O((\log N) N^{4/3})$$
$$+ O(\#\{x,y\in[-N,N] : \gcd(x,y)=1,\ \exists p > N^{4/3},\ p^2 \mid P(x,y)\}),$$

where the implied constants depend only on P, c_0, c_1 and c_2.

Proof. We define a soil $(\mathscr{P}, \mathscr{A}, r, f)$ by

$$\mathscr{P} = \{p \in \mathbb{Z}^+ : p \text{ prime}\}, \qquad \mathscr{A} = \{1 \le x, y \le N : \gcd(x,y) = 1\},$$
$$r((x,y)) = \{p \in \mathscr{P} : p^2 \mid P(x,y)\}, \qquad f((x,y),d) = \prod_{p\in d} u_p(x,y).$$

Let $h(d) = \prod_{p\in d} p^2$. Properties (h1) and (h2) are clear. Lemmas A.3 and A.5 give us property (A1) with

$$X = N^2 \prod_p \left(1 - \frac{1}{p^2}\right), \qquad C_0 \ll |\mathrm{Disc}\, P|^3, \qquad C_1, C_2 \ll \deg P.$$

Choose the sampling datum in Example 3 with $n = N$. Proceed as in Proposition 3.7. ■

It is simple to show that certain natural classes of functions u_p satisfy the conditions in Propositions 3.7 and 3.8.

LEMMA 3.9. *Let $P \in \mathbb{Z}[x]$ be a square-free polynomial. Let p be a rational prime. Let $u_p : \mathbb{Z}_p \to \mathbb{C}$ be such that $u_p(x)$ depends only on $x \bmod p$ and $v_p(P(x))$. Then u_p is $(c_0, c_1 p^{-c_2 j})$-approximable, where c_0, c_1 and c_2 depend only on P, not on p.*

Proof. Let $c_0 = 2|\mathrm{Disc}\, P|^3 \deg P$, $c_1 = |\mathrm{Disc}\, P|^3 \deg P$. Let $x_1, \ldots, x_c$ be the solutions to $P(x) \equiv 0 \bmod p$ in $\mathbb{Z}/p$. Clearly $c \leq \deg P$. Define

$$M_{p,j_0,j_1} = \{x \in \mathbb{Z}_p : v_p(P(x)) = j_0,\ x \equiv x_{j_1} \bmod p\}.$$

Let $M_{p,0} = \{x \in \mathbb{Z}_p : p \nmid P(x)\}$. We have a partition

$$\mathbb{Z}_p = M_{p,0} \cup M_{p,1,1} \cup \cdots \cup M_{p,1,c} \cup M_{p,2,1} \cup \cdots \cup M_{p,2,c} \cup \cdots.$$

By Lemma A.2,

$$M_{p,j_0,j_1} \in \mathscr{M}_{c_0,p}, \qquad \mu_p(M_{p,j_0,j_1}) \leq \mu_p(\{x \in \mathbb{Z}_p : v_p(P(x)) = j_0\}) \leq c_1 p^{-j_0}.$$

Let $c_2 = 1/\deg P$. Thus $c_2 \leq 1/c$. The statement follows. ∎

LEMMA 3.10. *Let $P \in \mathbb{Z}[x, y]$ be a square-free homogeneous polynomial. Let p be a rational prime. Let $u_p : \mathbb{Z}_p^2 - p\mathbb{Z}_p^2 \to \mathbb{C}$ be such that $u_p(x, y)$ depends only on $xy^{-1} \bmod p \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ and $v_p(P(x, y))$. Then u_p is $(c_0, c_1 p^{-c_2 j})$-approximable, where c_0, c_1 and c_2 depend only on P, not on p.*

Proof. Same as Lemma 3.9. ∎

3.5. *Averages with multipliers.* The framework developed in Section 3.3 involves two different sets of measures, $\{\mu_j\}$ and $\{\sigma_j\}$, which have been set equal in the above. The fact that $\{\mu_j\}$ and $\{\sigma_j\}$ can be taken to be different allows us to compute sums of the form $\sum s(n) \prod_p u_p(n)$, where $s(n)$ is a function as in Section 3.3—a good *multiplier*, if you wish.

The most natural non-trivial example may be $s(n) = \mu(n)$. The function $\mu(n)$ averages to zero over arithmetic progressions. More precisely,

$$\frac{1}{N/m} \sum_{\substack{1 \leq n \leq N \\ n \equiv a \bmod m}} \mu(n) \ll N e^{-C(\log N)^{2/3}/(\log\log N)^{1/5}} \tag{3.11}$$

for $m \leq (\log N)^A$, where both C and the implied constant depend only on A. We would like to show that $\mu(n) \prod_p u_p(n)$ averages to zero as well. The utility of such a result follows from the discussion around (3.2): we want to average a function of the form

$$W(\mathscr{E}(n)) = \prod_p W_{0,p}(\mathscr{E}(n)) \prod_p \frac{W_p(\mathscr{E}(n))}{W_{0,p}(\mathscr{E}(n))} = f(n) \prod_p u_p(n).$$

The factor $f(n)$ can generally be expressed in the form $\mu(P(n))g(n)$, where P is a polynomial (possibly constant) and $g(n)$ is a factor that can be absorbed into the local factors $u_p(n)$:

$$g(n)\prod_p u_p(n) = \prod_p u_{p,1}(n).$$

Thus, it befalls us to show that $\mu(P(n))\prod_p u_{p,1}(n)$ averages to zero. If P is linear, we may use (3.11) and Proposition 3.11 below; in general, Proposition 3.11 furnishes us with a result conditional on

$$\lim_{N\to\infty}\frac{1}{N}\,\mu(P(n)) = 0 \qquad \text{(Chowla's conjecture)}.$$

When we average $W_p(\mathscr{E}(t))$ over the rationals, we are computing

$$\sum_{\substack{1\le x,y\le N\\ \gcd(x,y)=1}} W(\mathscr{E}(x/y)),$$

or, in effect, the average of

$$\mu(P(x,y))\prod_p u_{p,1}(x,y).$$

For $\deg P = 1, 2$, we have an analogue of (3.11). For $\deg P = 3$, we know from [He2, Th. 3.7.1 and Lem. 2.4.4] that

$$\sum_{\substack{-N\le x,y\le N\\ (x,y)\in S\cap L\\ \gcd(x,y)=1}} \mu(P(x,y)) \ll \frac{(\log\log N)^6(\log\log\log N)}{\log N}\,\frac{N^2}{[\mathbb{Z}^2 : L]}$$

for every lattice L with $[\mathbb{Z}^2 : L] \le (\log N)^A$, where the implied constant depends only on A.

A good multiplier need not have average zero. A simple and useful example of a multiplier is given by the characteristic function of an arithmetic progression $a + \mathbb{Z}m$ or of a lattice coset $L \subset \mathbb{Z}^2$.

PROPOSITION 3.11. *For every prime p, let $u_p : \mathbb{Z}_p \to \mathbb{C}$ be a $(c_0, c_1 p^{-c_2 j})$-approximable function, where c_0 is a positive integer and c_1, c_2 are positive real numbers. Assume that $|u_p(x)| \le 1$ for every $x \in \mathbb{Z}_p$. Assume, furthermore, that $u_p(x) = 1$ unless $p^2 \mid P(x)$, where $P \in \mathbb{Z}[x]$ is a fixed square-free polynomial.*

Let $s : \mathbb{Z}^+ \to \mathbb{C}$ be a function with $|s(n)| \le 1$ for every $n \in \mathbb{Z}^+$. Let σ_p be a measure on $\mathbb{Z}_p$ with $\max_{S\subset\mathbb{Z}_p} |\sigma_p(S)/\mu_p(S)| \le 1$, where μ_p is the usual measure on $\mathbb{Z}_p$. Suppose there are $\varepsilon(N)$, $\eta(N)$ with $0 \le \varepsilon(N) \le 1$, $1 \le \eta(N) \le N$, such that

$$\sum_{\substack{1\le n\le N\\ n\equiv a \bmod m}} s(n) = N\prod_p \sigma_p(\{n\in\mathbb{Z}_p : n\equiv a \bmod p^{v_p(m)}\}) + O\left(\frac{\varepsilon(N)N}{m}\right) \tag{3.12}$$

for all a, m *with* $0 < m \le \eta(N)$. *Then*

$$\begin{aligned}\frac{1}{N}\sum_{n=1}^{N} s(n)\prod_p u_p(n) &= \prod_p \int_{\mathbb{Z}_p} u_p(x)\,d\sigma_p + O\left(\varepsilon(N) + \frac{1}{\eta(N)^{1/2-\varepsilon'}}\right)\\ &\quad + \frac{1}{N}O(\#\{1\le x\le N : \exists p > N^{1/2},\ p^2 \mid P(x)\})\end{aligned} \tag{3.13}$$

for all $\varepsilon' > 0$, *where the implied constant depends only on* P, c_0, c_1, c_2, ε', *and the implied constant in* (3.12).

Proof. Define a soil $(\mathscr{P},\mathscr{A},r,f)$ as in Proposition 3.7. Choose the sampling datum in Example 1 with $n = N$. Then (A2) holds with $g(d_1,d_2)$ as in Proposition 3.7 with σ_p instead of μ_p, and

$$\begin{aligned}r_{d_1,d_2} \le N \sum_{(s_j)\in(\mathbb{Z}^+)^{d_1}-S}\ \prod_{p\in d_1} m_p(s_p) + c_0^{\#d_1}\varepsilon(N)N\prod_{j\in d_1}\mu_j(M_j)\\ + (\#S)\frac{c_0^{\#d_1}N}{\eta(N)} + (\#S+1)c_0^{\#d_1}\end{aligned}$$

for every $S\in(\mathbb{Z}^+)^{d_1}$ and $m_p(j) = c_1 p^{-c_2 j}$. Choose

$$S = \bigtimes_{p\in d_1}\left\{n\in\mathbb{Z} : 1\le n\le \frac{c_2\log\eta(N)}{\log p}\right\}.$$

Then

$$\sum_{(s_j)\in(\mathbb{Z}^+)^{d_1}-S}\ \prod_{p\in d_1} m_p(s_p) \le \frac{c_1}{1-p^{-c_2}}\#d_1/\eta(N)$$

and

$$r_{d_1,d_2} \ll c_0^{\#d_1}\left(\frac{\varepsilon(N)N}{h(d_1)}(\deg P)^{\#d_1} + \frac{N}{\eta(N)}\#d_1 + \frac{N}{\eta(N)}\prod_{p\in d_1}\frac{c_2\log\eta(N)}{\log p}\right).$$

Apply Corollary 3.3. The first and second terms of (3.7) are as in Proposition 3.7. By Lemma B.1, the third term is

$$O\left(\varepsilon(N)N + \frac{NM^{1/2+\varepsilon'}}{\eta(N)^{1-\varepsilon'}}\right).$$

The fourth term is

$$\begin{aligned}\sum_{p>M} &\#\{1 \le x \le N : p^2 \mid P(x)\} \\ &= \sum_{M<p\le N^{1/2}} \#\{1 \le x \le N : p^2 \mid P(x)\} + \sum_{p>N^{1/2}} \#\{1 \le x \le N : p^2 \mid P(x)\} \\ &\ll \sum_{M<p\le N^{1/2}} N/p^2 + \#\{1 \le x \le N : \exists p > N^{1/2},\, p^2 \mid P(x)\} \\ &\le NM^{-1} + \#\{1 \le x \le N : \exists p > N^{1/2},\, p^2 \mid P(x)\}.\end{aligned}$$

Set $M = \eta(N)$. The result follows. ■

PROPOSITION 3.12. *For every* p, *let* $u_p : \mathbb{Z}_p^2 - p\mathbb{Z}_p^2 \to \mathbb{C}$ *be a* $(c_0, c_1 p^{-c_2})$-*approximable function, where* c_0 *is a positive integer and* c_1, c_2 *are positive real numbers. Assume that* $|u_p(x,y)| \le 1$ *for all* $(x,y) \in \mathbb{Z}_p^2 - p\mathbb{Z}_p^2$. *Assume, furthermore, that* $u_p(x,y) = 1$ *for all* $(x,y) \in \mathbb{Z}_p^2 - p\mathbb{Z}_p^2$ *such that* $p^2 \nmid P(x)$, *where* $P \in \mathbb{Z}[x,y]$ *is a fixed square-free homogeneous polynomial.*

Let $S \subset \mathbb{R}^2$ *be a sector. Let* $s : \{(x,y) \in \mathbb{Z}^2 : \gcd(x,y) = 1\} \to \mathbb{C}$ *be a function with* $|s(x,y)| \le 1$ *for all* $x, y \in \mathbb{Z}$, $\gcd(x,y) = 1$. *Let* σ_p *be a measure on* $\mathbb{Z}_p^2 - p\mathbb{Z}_p^2$ *with* $\max_{S\subset \mathbb{Z}_p^2 - p\mathbb{Z}_p^2} |\sigma_p(S)/\mu_p(S)| \le 1$, *where* μ_p *is the usual measure on* $\mathbb{Z}_p^2$. *Suppose there are* $\varepsilon(N)$, $\eta(N)$ *with* $0 \le \varepsilon(N) \le 1$, $1 \le \eta(N) \le N$, *such that*

$$\sum_{\substack{-N\le x,y\le N\\ (x,y)\in S\cap L\\ \gcd(x,y)=1}} s(x,y) = N^2 \prod_p \sigma_p(\{(x,y) \in (\mathbb{Z}_p^2 - p\mathbb{Z}_p^2) \cap L_p\}) + O\left(\frac{\varepsilon(N)N}{[\mathbb{Z}^2 : L]}\right) \tag{3.14}$$

for all lattices $L \subset \mathbb{Z}^2$ *with* $[\mathbb{Z}^2 : L] \ll \eta(N)$, *where* $L_p \subset \mathbb{Z}_p^2$ *is the additive subgroup of* $\mathbb{Z}_p^2$ *generated by* $\mathbb{Z}_p L$. *Then*

$$\begin{aligned}\frac{1}{N^2} \sum_{\substack{-N\le x,y\le N\\ (x,y)\in S\\ \gcd(x,y)=1}} s(x,y) \prod_p u_p(x,y) &= \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} u_p(x,y)\, d\sigma_p + O\left(\varepsilon(N) + \frac{1}{\eta(N)^{1/2-\varepsilon'}}\right) \\ &\quad + \frac{1}{N^2} O(\#\{-N \le x,y \le N : \gcd(x,y) = 1,\, \exists p > N,\, p^2 \mid P(x,y)\})\end{aligned} \tag{3.15}$$

for all $\varepsilon' > 0$, *where the implied constant depends only on* P, c_0, c_1, c_2, ε', *and the implied constant in* (3.14).

Proof. As in Proposition 3.11. Use Proposition 3.8 instead of 3.7. ■

The reader may wonder why Proposition 3.11 requires information on averages on arithmetic progressions (3.12), yet seems to furnish data only on averages over all positive integers (3.13). In fact, we can obtain information on averages over arithmetic progressions by applying Proposition 3.11 to a new multiplier s_0 defined in terms of a given arithmetic progression $a+m\mathbb{Z}$:

$$s_0(n) = \begin{cases} s(n) & \text{if } n \equiv a \bmod m, \\ 0 & \text{otherwise.} \end{cases}$$

The same can be done as far as Proposition 3.12 and equations (3.14) and (3.15) are concerned, with lattice and lattice cosets playing the role of arithmetic progressions.

4. Large square divisors of values of polynomials. It is now time to estimate the error terms denoted by $\delta(N)$ in the introduction. These are error terms of the form

$$\frac{1}{N} O(\#\{1 \le x \le N : \exists p > N^{1/2},\, p^2 \mid P(x)\}$$

and

$$\frac{1}{N^2} O(\#\{-N \le x, y \le N : \gcd(x,y) = 1,\, \exists p > N,\, p^2 \mid P(x,y)\}),$$

where $P \in \mathbb{Z}[x]$ (resp. $P \in \mathbb{Z}[x,y]$ homogeneous) is a given polynomial square-free as an element of $\mathbb{Q}[x]$ (resp. square-free as an element of $\mathbb{Q}[x,y]$). In order to go beyond previous estimates, we will need to go beyond sieve theory into Diophantine geometry.

4.1. *Elliptic curves, heights and lattices.* As is usual, we write $\widehat{h}$ for the canonical height on an elliptic curve E, and h_x, h_y for the height on E with respect to x, y:

$$h_x((x,y)) = \begin{cases} 0 & \text{if } P = O, \\ \log H(x) & \text{if } P = (x,y), \end{cases}$$

$$h_y((x,y)) = \begin{cases} 0 & \text{if } P = O, \\ \log H(y) & \text{if } P = (x,y), \end{cases}$$

where O is the origin of E, taken to be the point at infinity, and

$$H(y) = (H_K(y))^{1/[K:\mathbb{Q}]}, \qquad H_K(y) = \prod_v \max(|y|_v^{n_v}, 1),$$

where K is any number field containing y, the product $\prod_v$ is taken over all places v of K, and n_v denotes the degree of $K_v/\mathbb{Q}_v$.

In particular, if x is a rational number x_0/x_1, $\gcd(x_0,x_1) = 1$, then

$$H(x) = H_{\mathbb{Q}}(x) = \max(|x_0|, |x_1|), \qquad h_x((x,y)) = \log(\max(|x_0|, |x_1|)).$$

The differences $\left|\widehat{h} - \frac{1}{2}h_x\right|$ and $\left|\widehat{h} - \frac{1}{3}h_y\right|$ are bounded on the set of all points of E (not merely on $E(\mathbb{Q})$). This basic property of the canonical height will be crucial in our analysis.

LEMMA 4.1. *Let $f \in \mathbb{Z}[x]$ be a cubic polynomial of non-zero discriminant. For every square-free rational integer d, let E_d be the elliptic curve*

$$E_d: \ dy^2 = f(x).$$

Let $P = (x, y) \in E_d(\mathbb{Q})$. Consider the point $P' = (x, d^{1/2}y)$ on E_1. Then $\widehat{h}(P) = \widehat{h}(P')$, where the canonical heights are defined on E_d and E_1, respectively,

Proof. Clearly $h_x(P') = h_x(P)$. Moreover $(P+P)' = P' + P'$. Hence

$$\widehat{h}(P) = \frac{1}{2}\lim_{N\to\infty} 4^{-N} h_x([2^N]P) = \frac{1}{2}\lim_{N\to\infty} 4^{-N} h_x([2^N]P') = \widehat{h}(P'). \ \blacksquare$$

LEMMA 4.2. *Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial. Let C be the curve given by $C: y^2 = f(x)$. Let $d \in \mathbb{Z}$ be square-free. Let x, y be rational numbers, $y \neq 0$, such that $P = (x, d^{1/2}y)$ lies on E. Then*

$$h_y(P) = \log H(d^{1/2}y) \leq \frac{3}{8}\log|d| + C_f,$$

where C_f is a constant depending only on f.

Proof. Write $y = y_0/y_1$, where y_0 and y_1 are coprime integers. Then

$$H(y) = \max\left(\frac{|y_0|\,|d|^{1/2}}{\sqrt{\gcd(d, y_1^2)}}, \frac{|y_1|}{\sqrt{\gcd(d, y_1^2)}}\right). \tag{4.1}$$

Write a for the leading coefficient of f. Let $p \mid \gcd(d, y_1^2)$, $p \nmid a$. Since d is square-free, $p^2 \nmid \gcd(d, y^2)$. Suppose $p^2 \nmid y_1$. Then $\nu_p(dy^2) = -1$. However, $dy^2 = f(x)$ implies that, if $\nu_p(x) \geq 0$, then $\nu_p(dy^2) \geq 0$, and if $\nu_p(x) < 0$, then $\nu_p(dy^2) \leq -3$. Contradiction. Hence $p \mid \gcd(d, y_1^2)$, $p \nmid a$ imply $p^2 \nmid \gcd(d, y_1^2)$, $p^2 \mid y_1$. Therefore $|y_1| \geq (\gcd(d, y_1^2)/a)^2$.

By (4.1) it follows that

$$\begin{aligned} H(P) &\geq \max\left(\frac{|d|^{1/2}}{\sqrt{\gcd(d, y_1^2)}}, \frac{|y_1|}{\sqrt{\gcd(d, y_1^2)}}\right) \\ &\geq \max\left(\frac{|d|^{1/2}}{\sqrt{\gcd(d, y_1^2)}}, \frac{(\gcd(d, y_1^2))^{3/2}}{a^2}\right). \end{aligned}$$

Since $\max(|d|^{1/2}z^{-1/2}, z^{3/2}/a^2)$ is minimal when $|d|^{1/2}z^{-1/2} = z^{3/2}/a^2$, i.e., when $z = a|d|^{1/4}$, we obtain

$$H(P) \geq |d|^{3/8}|a|^{-1/2}.$$

Hence

$$h_y(P) = \log H(P) \geq \frac{3}{8}\log|d| - \frac{1}{2}\log|a|. \ \blacksquare$$

Corollary 4.3. *Let $f \in \mathbb{Z}[x]$ be a cubic polynomial of non-zero discriminant. For every square-free rational integer d, let E_d be the elliptic curve*

$$E_d : \ dy^2 = f(x).$$

Let $P = (x, y) \in E_d(\mathbb{Q})$. Then

$$\widehat{h}(P) \geq \frac{1}{8} \log |d| + C_f,$$

where C_f is a constant depending only on f.

Proof. Let $P' = (x, d^{1/2}y) \in E_1$. By Lemma 4.1, $\widehat{h}(P) = \widehat{h}(P')$. The difference $|\widehat{h} - h_x|$ is bounded on E. The statement follows from Lemma 4.2. ∎

The following crude estimate will suffice for some of our purposes.

Lemma 4.4. *Let Q be a positive definite quadratic form on $\mathbb{Z}^r$. Suppose $Q(\vec{x}) \geq c_1$ for all non-zero $\vec{x} \in \mathbb{Z}^r$. Then there are at most $(1 + 2\sqrt{c_2/c_1})^r$ values of $\vec{x}$ for which $Q(\vec{x}) \leq c_2$.*

Proof. There is a linear bijection $f : \mathbb{Q}^r \to \mathbb{Q}^r$ taking Q to the square root of the Euclidean norm: $Q(\vec{x}) = |f(\vec{x})|^2$ for all $\vec{x} \in \mathbb{Q}^r$. Because $Q(\vec{x}) > c_1$ for all non-zero $\vec{x} \in \mathbb{Z}^r$, we see that $f(\mathbb{Z}^r)$ is a lattice $L \subset \mathbb{Q}^r$ such that $|\vec{x}| \geq c_1^{1/2}$ for all $\vec{x} \in L$, $\vec{x} \neq 0$. We can draw a sphere $S_{\vec{x}}$ of radius $\frac{1}{2}c_1^{1/2}$ around each point $\vec{x}$ of L. The spheres do not overlap. If $\vec{x} \in L$, $|\vec{x}| \in c_2^{1/2}$, then $S_{\vec{x}}$ is contained in the sphere S' of radius $c_2^{1/2} + c_1^{1/2}/2$ around the origin. The total volume of all spheres $S_{\vec{x}}$ within S' is no greater than the volume of S'. Hence

$$(\#\{\vec{x} \in L : |\vec{x}| \leq c_2^{1/2}\})(c_1^{1/2}/2)^r \leq (c_2^{1/2} + c_1^{1/2}/2)^r.$$

The statement follows. ∎

Corollary 4.5. *Let E be an elliptic curve over $\mathbb{Q}$. Suppose there are no non-torsion points $P \in E(\mathbb{Q})$ of canonical height $\widehat{h}(P) < c_1$. Then there are at most $O((1 + 2\sqrt{c_2/c_1})^{\operatorname{rank}(E)})$ points $P \in E(\mathbb{Q})$ for which $\widehat{h}(P) < c_2$. The implied constant is absolute.*

Proof. The canonical height $\widehat{h}$ is a positive-definite quadratic form on the free part $\mathbb{Z}^{\operatorname{rank}(E)}$ of $E(\mathbb{Q}) \sim \mathbb{Z}^{\operatorname{rank}(E)} \times T$. A classical theorem of Mazur's [Maz] states that the cardinality of T is at most 16. Apply Lemma 4.4. ∎

Note that we could avoid the use of Mazur's theorem, since Lemmas 4.1 and 4.2 imply that the torsion group of E_d is either $\mathbb{Z}/2$ or trivial for large enough d.

4.2. *Twists of cubics and quartics.* Let $f(x) = a_4x^4+a_3x^3+a_2x^2+a_1x+a_0 \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 4. For every square-free $d \in \mathbb{Z}$, consider the curve

$$C_d: \ dy^2 = f(x). \tag{4.2}$$

If there is a rational point (r, s) on C_d, then there is a birational map from C_d to the elliptic curve

$$E_d: \ dy^2 = x^3 + a_2x^2 + (a_1a_3 - 4a_0a_4)x - (4a_0a_2a_4 - a_1^2a_4 - a_0a_3^2). \tag{4.3}$$

Moreover, we can construct such a birational map in terms of (r, s) as follows. Let (x, y) be a rational point on C_d. We can rewrite (4.2) as

$$y^2 = \frac{1}{d} f(x).$$

We change variables:

$$x_1 = x - r, \qquad y_1 = y$$

satisfy

$$y^2 = \frac{1}{d}\left(\frac{1}{4!} f^{(4)}(r)x_1^4 + \frac{1}{3!} f^{(3)}(r)x_1^3 + \frac{1}{2!} f''(r)x_1^2 + \frac{1}{1!} f'(r)x_1 + f(r)\right).$$

We now apply the standard map for putting quartics in Weierstrass form:

$$x_2 = (2s(y_1 + s) + f'(r)x_1/d)/x_1^2,$$
$$y_2 = (4s^2(y_1 + s) + 2s(f'(r)x_1/d + f''(r)x_1^2/(2d)) - (f'(r)/d)^2x_1^2/(2s))/x_1^3$$

satisfy

$$y_2^2 + A_1x_2y_2 + A_3y_2 = x_2^3 + A_2x_2^2 + A_4x_2 + A_6 \tag{4.4}$$

with

$$A_1 = \frac{1}{d} f'(r)/s, \qquad A_2 = \frac{1}{d} (f''(r)/2 - (f'(r))^2/(4f(r))),$$
$$A_3 = \frac{2s}{d} f^{(3)}(r)/3!, \qquad A_4 = -\frac{1}{d^2} \cdot 4f(r) \cdot \frac{1}{4!} f^{(4)}(r),$$
$$A_6 = A_2A_4.$$

To take (4.4) to E_d, we apply a linear change of variables:

$$x_3 = dx_2 + r(a_3 + 2a_4r), \qquad y_2 = \frac{d}{2} (2y_2 + a_1x_2 + a_3)$$

satisfy

$$dy_3^2 = x_3^3 + a_2x_3^2 + (a_1a_3 - 4a_0a_4)x_3 - (4a_0a_2a_4 - a_1^2a_4 - a_0a_3^2).$$

We have constructed a birational map $\phi_{r,s}(x, y) \mapsto (x_3, y_3)$ from C_d to E_d.

Now consider the equation

$$dy^2 = a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4. \tag{4.5}$$

Suppose there is a solution (x_0, y_0, z_0) to (4.5) with $x_0, y_0, z_0 \in \mathbb{Z}$, $|x_0|, |z_0| \leq N$, $z_0 \neq 0$. Then $(x_0/z_0, y_0/z_0^2)$ is a rational point on (4.2). We can set

$r = x_0/z_0$, $s = y_0/z_0^2$ and define a map $\phi_{r,s}$ from C_d to E_d as above. Now let $x, y, z \in \mathbb{Z}$, $|x|, |z| \le N$, $z_0 \ne 0$, be another solution to (4.5). Then

$$P = \phi_{r,s}(x_0/z_0, y_0/z_0^2)$$

is a rational point on E_d. Notice that $|y_0|, |y| \ll (N^4/d)^{1/2}$. Write

$$\phi_{r,s}(P) = (u_0/u_1, v),$$

where $u_0, u_1 \in \mathbb{Z}$, $v \in \mathbb{Q}$, $\gcd(u_0, u_1) = 1$. By a simple examination of the construction of $\phi_{r,s}$ we can determine that $\max(u_0, u_1) \ll N^7$, where the implied constant depends only on $a_0, a_1, \ldots, a_4$. In other words,

$$h_x(P) \le 7 \log N + C, \tag{4.6}$$

where C is a constant depending only on a_j. Notice that (4.6) holds even for $(x, y, z) = (x_0, y_0, z_0)$, as then P is the origin of E.

The value of $h_x(P)$ is independent of whether P is considered as a rational point of E_d or as a point of E_1. Let $\widehat{h}_{E_1}(P)$ be the canonical height of P as a point of E_1. Then

$$\left| \widehat{h}_{E_1}(P) - \frac{1}{2} h_x(P) \right| \le C',$$

where C' depends only on f. By Lemma 4.1, the canonical height $\widehat{h}_{E_1}(P)$ of P as a point of E_1 equals the canonical height $\widehat{h}_{E_d}(P)$ of P as a point of E_d. Hence

$$\left| \widehat{h}_{E_d}(P) - \frac{1}{2} h_x(P) \right| \le C'.$$

Then, by (4.6),

$$\widehat{h}_{E_d}(P) \le \frac{7}{2} \log N + (C/2 + C').$$

We have proven

Lemma 4.6. *Let $f(x,z) = a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4 \in \mathbb{Z}[x,z]$ be an irreducible homogeneous polynomial. Then there is a constant C_f such that the following holds. Let N be any positive integer. Let d be any square-free integer. Let $S_{d,1}$ be the set of all solutions $(x, y, z) \in \mathbb{Z}^3$ to*

$$dy^2 = f(x, z)$$

satisfying $|x|, |z| \le N$, $\gcd(x, z) = 1$. Let $S_{d,2}$ be the set of all rational points P on

$$E_d : \ dy^2 = x^3 + a_2x^2 + (a_1a_3 - 4a_0a_4)x - (4a_0a_2a_4 - a_1^2a_4 - a_0a_3^2) \tag{4.7}$$

with canonical height

$$\widehat{h}(P) \le \frac{7}{2} \log N + C_f.$$

Then there is an injective map from $S_{d,1}$ to $S_{d,2}$.

We can now apply the results of Subsection 4.1.

PROPOSITION 4.7. *Let* $f(x,z) = a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4 \in \mathbb{Z}[x,z]$ *be an irreducible homogeneous polynomial. Then there are constants* $C_{f,1}$, $C_{f,2}$, $C_{f,3}$ *such that the following holds. Let* N *be any positive integer. Let* d *be any square-free integer. Let* S_d *be the set of all solutions* $(x,y,z) \in \mathbb{Z}^3$ *to*

$$dy^2 = f(x,z)$$

satisfying $|x|, |z| \leq N$, $\gcd(x,z) = 1$. *Then*

$$\#S_d \ll \begin{cases} \left(1 + 2\sqrt{\left(\frac{7}{2}\log N + C_{f,1}\right)/\left(\frac{1}{8}\log|d| + C_{f,2}\right)}\right)^{\operatorname{rank}(E_d)} & \text{if } |d| \geq C_{f,4}, \\ \left(1 + 2C_{f,3}\sqrt{\frac{7}{2}\log N + C_{f,1}}\right)^{\operatorname{rank}(E_d)} & \text{if } |d| < C_{f,4}, \end{cases}$$

where $C_{f,4} = e^{9C_{f,2}}$, E_d *is as in* (4.7), *and the implied constant depends only on* f.

Proof. If $|d| \leq C_{f,4}$, apply Corollary 4.5 and Lemma 4.6. If $|d| > C_{f,4}$, apply Corollary 4.3, Corollary 4.5 and Lemma 4.6. ■

4.3. *Divisor functions and their averages.* As is usual, we denote by $\omega(d)$ the number of prime divisors of a positive integer d. Given an extension $K/\mathbb{Q}$, we define

$$\omega_K(d) = \sum_{\substack{\mathfrak{p} \in I_K \\ \mathfrak{p} | d}} 1.$$

LEMMA 4.8. *Let* $f(x) \in \mathbb{Z}[x]$ *be an irreducible polynomial of degree* 3 *and non-zero discriminant. Let* $K = \mathbb{Q}(\alpha)$, *where* α *is a root of* $f(x) = 0$. *For every square-free rational integer* d, *let* E_d *be the elliptic curve given by*

$$dy^2 = f(x).$$

Then

$$\operatorname{rank}(E_d) = C_f + \omega_K(d) - \omega(d),$$

where C_f *is a constant depending only on* f.

Proof. Write $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$. Let $f_d(x) = a_3x^3 + da_2x^2 + d^2a_1x + d^3a_0$. Then $d\alpha$ is a root of $f_d(x) = 0$. Clearly $\mathbb{Q}(d\alpha) = \mathbb{Q}(\alpha)$. If p is a prime of good reduction for E_1, then E_d will have additive reduction at p if $p \mid d$, and good reduction at p if $p \nmid d$. The statement now follows immediately from the standard bound in [BK, Prop. 7.1]. ■

If $dy^2 = f(x)$ is to have any integer points $(x,y) \in \mathbb{Z}^2$ at all, no prime unsplit in $\mathbb{Q}(\alpha)/\mathbb{Q}$ can divide d. We define

$$R(\alpha, d) = \begin{cases} 2^{\alpha\omega_{\mathbb{Q}(\alpha)}(d) - \alpha\omega(d)} & \text{if no } p \mid d \text{ is unsplit}, \\ 0 & \text{otherwise}. \end{cases} \tag{4.8}$$

LEMMA 4.9. *Let $K/\mathbb{Q}$ be a non-Galois extension of $\mathbb{Q}$ of degree 3. Let $L/\mathbb{Q}$ be the normal closure of $K/\mathbb{Q}$. Let p be a rational prime that does not ramify in $L/\mathbb{Q}$. Then p splits completely in $K/\mathbb{Q}$ if and only if it splits completely in $L/\mathbb{Q}$.*

Proof. If $\mathrm{Frob}_p = \{I\}$, then p splits completely in $K/\mathbb{Q}$ and in $L/\mathbb{Q}$. Suppose $\mathrm{Frob}_p \neq \{I\}$. Then p does not split completely in $L/\mathbb{Q}$. Since only one map in $\mathrm{Gal}(L/\mathbb{Q})$ other than the identity fixes $K/\mathbb{Q}$, and every conjugacy class in $\mathrm{Gal}(L/\mathbb{Q})$ has more than one element, there must be a map $\phi \in \mathrm{Frob}_p$ that does not fix $K/\mathbb{Q}$. Hence p does not split completely in $K/\mathbb{Q}$. ■

LEMMA 4.10. *Let $K/\mathbb{Q}$ be an extension of $\mathbb{Q}$ of degree 3. Let α be a positive real number. Let $S_\alpha(X) = \sum_{n\le X} R(\alpha, n)$. Then*

$$S_\alpha(X) \sim \begin{cases} C_{K,\alpha} X (\log X)^{\frac{1}{3}2^{2\alpha}-1} & \text{if } K/\mathbb{Q} \text{ is Galois},\\ C_{K,\alpha} X (\log X)^{\frac{1}{2}2^{\alpha}+\frac{1}{6}2^{2\alpha}-1} & \text{if } K/\mathbb{Q} \text{ is not Galois},\end{cases} \tag{4.9}$$

where $C_{K,\alpha} > 0$ depends only on K and α, and the dependence of $C_{K,\alpha}$ on α is continuous.

Proof. Suppose $K/\mathbb{Q}$ is Galois. Then, for $\Re(s) > 1$,

$$\begin{aligned}\zeta_{K/\mathbb{Q}}(s) &= \prod_{\mathfrak{p}\in I_K} \frac{1}{1-(N\mathfrak{p})^{-s}}\\ &= \prod_{p \text{ ramified}} \frac{1}{1-p^{-s}} \prod_{\substack{p \text{ unsplit}\\ \& \text{ unramified}}} \frac{1}{1-p^{-3s}} \prod_{p \text{ split}} \frac{1}{(1-p^{-s})^3}.\end{aligned}$$

Hence

$$\prod_{p \text{ split}} (1+\beta p^{-s}) = L_1(s)(\zeta_{K/\mathbb{Q}}(s))^{\beta/3}, \tag{4.10}$$

where $L_1(s)$ is holomorphic and bounded on $\{s : \Re(s) > 1/2 + \varepsilon\}$. Since

$$\sum_n R(\alpha, n) n^{-s} = \sum_{\substack{n\\ p|n \Rightarrow p \text{ split}}} 2^{2\alpha} n^{-s} = \prod_{p \text{ split}} (1 + 2^{2\alpha}p^{-s} + 2^{2\alpha}p^{-2s} + \cdots),$$

it follows that

$$\sum_n R(\alpha, n) = L_1(s)(\zeta_{K/\mathbb{Q}}(s))^{2^{2\alpha}/3}.$$

By a Tauberian theorem (see, e.g., [PT, Main Th.]) we can conclude that

$$\frac{1}{X}\sum_{n\le X} R(\alpha, n) \sim C_{K,\alpha}(\log X)^{\frac{1}{3}2^{2\alpha}-1}$$

for some positive constant $C_{K,\alpha} > 0$.

Now suppose that $K/\mathbb{Q}$ is not Galois. Denote the splitting type of a prime p in $K/\mathbb{Q}$ by $p = \mathfrak{p}_1\mathfrak{p}_2$, $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $p = \mathfrak{p}_1^2\mathfrak{p}_2$, etc. Let $L/\mathbb{Q}$ be the Galois closure of $K/\mathbb{Q}$. By Lemma 4.9,

$$\begin{aligned}\zeta_{K/\mathbb{Q}}(s) &= \prod_{\mathfrak{p}\in I_K} \frac{1}{1-(N\mathfrak{p})^{-s}}\\ &= L_2(s) \prod_{p=\mathfrak{p}_1\mathfrak{p}_2} \frac{1}{(1-p^{-s})} \prod_{p=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \frac{1}{(1-p^{-s})^3},\\ \zeta_{L/\mathbb{Q}}(s) &= \prod_{\mathfrak{p}\in I_L} \frac{1}{1-(N\mathfrak{p})^{-s}} = L_3(s) \prod_{p=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \frac{1}{(1-p^{-s})^6},\end{aligned} \tag{4.11}$$

where $L_2(s)$ and $L_3(s)$ are continuous, non-zero and bounded on $\{s : \Re(s) > 1/2\}$. Thus

$$\begin{aligned}\sum_n R(\alpha,n)n^{-s} &= \prod_{p=\mathfrak{p}_1\mathfrak{p}_2} (1+2^\alpha p^{-s}) \prod_{p=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} (1+2^{2\alpha}p^{-s})\\ &= L_4(s)\zeta_{K/\mathbb{Q}}(s)^{2^\alpha} \zeta_{L/\mathbb{Q}}^{-\frac{1}{2}2^\alpha+\frac{1}{6}2^{2\alpha}}.\end{aligned}$$

Since $\zeta_{K/\mathbb{Q}}$ and $\zeta_{L/\mathbb{Q}}$ both have a pole of order 1 at $s = 1$, we can apply a Tauberian theorem as before, obtaining

$$\frac{1}{X}\sum_{n\leq X} R(\alpha,n) \sim C_{K,\alpha}(\log X)^{\frac{1}{2}2^\alpha+\frac{1}{6}2^{2\alpha}-1}. \blacksquare$$

4.4. *The square-free sieve for homogeneous quartics.* We need the following simple lemma. See Lemma A.5 for a related statement.

LEMMA 4.11. *Let $f \in \mathbb{Z}[x,z]$ be a homogeneous polynomial. Then there is a constant C_f such that the following holds. Let N be a positive integer larger than C_f. Let p be a prime larger than N. Then there are at most $12\deg(f)$ pairs $(x,z) \in \mathbb{Z}^2$, $|x|,|z| \leq N$, $\gcd(x,z) = 1$, such that*

$$p^2 \mid f(x,z). \tag{4.12}$$

Proof. If N is large enough, then p does not divide the discriminant of f. Hence

$$f(r,1) \equiv 0 \bmod p^2 \tag{4.13}$$

has at most $\deg(f)$ solutions in $\mathbb{Z}/p^2$. If N is large enough for p^2 not to divide the leading coefficients of f, then $(x,z) = (1,0)$ does not satisfy (4.12). Therefore, any solution (x,z) to (4.12) gives us a solution $r = x/z$ to (4.13). We can focus on solutions $(x,z) \in \mathbb{Z}^2$ to (4.12) with x, z non-negative, as we need only flip signs to repeat the procedure for the other quadrants.

Suppose we have two solutions $(x_0, z_0), (x_1, z_1) \in \mathbb{Z}^2$ to (4.12) such that

$$\begin{aligned} &0 \le |x_0|, |x_1|, |z_0|, |z_1| \le N, \\ &\gcd(x_0, z_0) = \gcd(x_1, z_1) = 1, \\ &x_0/z_0 \equiv r \equiv x_1/z_1 \bmod p^2. \end{aligned}$$

Then

$$x_0 z_1 - x_1 z_0 \equiv 0 \bmod p^2.$$

Since $0 \le x_j, z_j \le N$ and $p > N$, we have

$$-p^2 < x_0 z_1 - x_1 z_0 < p^2,$$

and thus $x_0 z_1 - x_1 z_0$ must be zero. Hence $x_0/z_0 = x_1/z_1$. Since $\gcd(x_0, z_0) = \gcd(x_1, z_1) = 1$ and $\operatorname{sgn}(x_0) = \operatorname{sgn}(x_1)$, it follows that $(x_0, z_0) = (x_1, z_1)$. ∎

REMARK. It was pointed out by Ramsay [Ra] that an idea akin to that in Lemma 4.11 suffices to improve Greaves's bound for homogeneous sextics [Gre] from $\delta(N) = N^2(\log N)^{-1/3}$ to $\delta(N) = N^2(\log N)^{-1/2}$.

PROPOSITION 4.12. *Let $f \in \mathbb{Z}[x, z]$ be a homogeneous irreducible polynomial of degree* 4. *Let*

$$\delta(N) = \#\{x, z \in \mathbb{Z}^2 : |x|, |z| \le N,\ \gcd(x, z) = 1,\ \exists p > N,\ p^2 \mid f(x, z)\}.$$

Then

$$\delta(N) \ll N^{4/3}(\log N)^A,$$

where A and the implied constant depend only on f.

Proof. Write $A = \max_{|x|,|z| \le N} f(x, z)$. Clearly $A \ll N^4$. We can write

$$\begin{aligned} \delta(N) \le \sum_{0<|d|\le M} &\#\{x, y, z \in \mathbb{Z}^3 : |x|, |z| \le N,\ \gcd(x, z) = 1,\ dy^2 = f(x, z)\} \\ &+ \sum_{N<p\le\sqrt{A/M}} \#\{x, z \in \mathbb{Z}^2 : |x|, |z| \le N,\ \gcd(x, z) = 1,\ p^2 \mid f(x, z)\}. \end{aligned}$$

Let $M \le N^3$. By Lemma 4.11,

$$\sum_{N<p\le\sqrt{A/M}} \#\{x, z \in \mathbb{Z}^2 : |x|, |z| \le N,\ \gcd(x, z) = 1,\ p^2 \mid f(x, z)\}$$

is at most a constant times $(\log N)^{-1}\sqrt{N^{4-\beta}}$, where $\beta = (\log M)/(\log N)$.

It remains to estimate $\sum_{0<|d|\le M} S(d)$, where we write

$$S(d) = \#\{x, y, z \in \mathbb{Z}^3 : |x|, |z| \le N,\ \gcd(x, z) = 1,\ dy^2 = f(x, z)\}.$$

Let $C_{f,1}$, $C_{f,2}$, $C_{f,3}$, $C_{f,4}$ be as in Proposition 4.7. Let K, C_f, ω and ω_K be as in Lemma 4.8. Write $C_{f,5}$ for C_f.

By Proposition 4.7,

$$\sum_{0<|d|<C_{f,4}} S(d) \ll \left(1+2C_{f,3}\sqrt{\frac{7}{2}\log N + C_{f,1}}\right)^{C_1} \ll (\log N)^{C_2},$$

where $C_1 = \max_{0<d<C_{f,4}} \operatorname{rank}(E_d)$, C_2 and the implied constant depend only on f. Let ε be a small positive real number. By Proposition 4.7 and Lemma 4.8,

$$\sum_{C_{f,4}\le|d|<N^\varepsilon} S(d) \ll \sum_{C_{f,4}\le|d|<N^\varepsilon} \left(1+2\sqrt{\frac{7}{2}\log N + C_{f,1}}\right)^{\operatorname{rank}(E_d)}$$
$$\ll \sum_{C_{f,4}\le|d|<N^\varepsilon} \left(1+2\sqrt{\frac{7}{2}\log N + C_{f,1}}\right)^{C_{f,5}+\omega_K(d)-\omega(d)}.$$

We have the following crude bounds:

$$\omega(d) \le \frac{\log|d|}{\log\log|d|}, \qquad \omega_K(d) \le 3\omega(d). \tag{4.14}$$

Hence

$$\sum_{C_{f,4}\le|d|<N^\varepsilon} S(d) \ll \sum_{C_{f,4}\le d<N^\varepsilon} (\log N)^{C_{f,5}+2\log d/\log\log d}$$
$$\le N^\varepsilon(\log N)^{C_1}(\log N)^{2\varepsilon\log N/\log\log N} \le (\log N)^{C_1}N^{3\varepsilon},$$

where C depends only on f and ε. For any d with $|d| > N^\varepsilon$, Proposition 4.7 and Lemma 4.8 give us

$$S(d) \ll \left(1+2\sqrt{\left(\frac{7}{2}\log N + C_{f,1}\right)\Big/\left(\frac{1}{8}\,\varepsilon\log N + C_{f,2}\right)}\,\right)^{\operatorname{rank}(E_d)}$$
$$\ll (12\varepsilon^{-1/2})^{C_{f,5}+\omega_K(d)-\omega(d)} \le 2^{C_2\omega_K(d)-C_2\omega_K(d)},$$

where C_2 depends only on f and ε. By Lemma 4.10 we can conclude that

$$\sum_{N^\varepsilon<|d|\le M} S(d) \ll \sum_{d=1}^{M} 2^{C_2\omega_K(d)-C_2\omega_K(d)} \ll C_3M(\log N)^{C_4},$$

where C_3 and C_4 depend only on f and ε. Set $M = N^{4/3}$, $\varepsilon = 1/4$. ∎

4.5. *Homogeneous cubics*

PROPOSITION 4.13. *Let $f \in \mathbb{Z}[x,z]$ be a homogeneous irreducible polynomial of degree* 3. *Let*

$$\delta(N) = \#\{x, z \in \mathbb{Z}^2 : |x|, |z| \le N,\ \gcd(x,z) = 1,\ \exists p > N,\ p^2 \mid f(x,z)\}.$$

Then

$$\delta(N) \ll N^{4/3}(\log N)^A,$$

where A and the implied constant depend only on f.

Proof. Write $A = \max_{|x|,|z|\le N} f(x,z)$. Clearly $A \ll N^4$. We can write

$$\delta(N) \le \sum_{0<|d|\le M} \#\{x,y,z \in \mathbb{Z}^3 : |x|,|z| \le N,\ \gcd(x,z)=1,\ dy^2 = f(x,z)\}$$
$$+ \sum_{N<p\le\sqrt{A/M}} \#\{x,z \in \mathbb{Z}^2 : |x|,|z| \le N,\ \gcd(x,z)=1,\ p^2 \mid f(x,z)\}.$$

Let $M \le N^2$. By Lemma 4.11, the second term on the right is at most a constant times $N^{2-\beta/2}/\log N$. Now notice that any point $(x,y,z) \in \mathbb{Z}^3$ on $dy^2 = f(x,z)$ gives us a rational point $(x',y') = (x/z, y/z^2)$ on

$$d'y'^2 = f(x',1), \tag{4.15}$$

where $d' = dz$. Moreover, a rational point on (4.15) can arise from at most one point $(x,y,z) \in \mathbb{Z}^3$, $\gcd(x,z)=1$, in the given fashion.

If $d \le M$, then $|d'| = |dz| \le MN$. The height $h_x(P)$ of the point $P = (x/z, y/z^2)$ is at most N. It follows by Lemma 4.1 that $\widehat{h}(P) \le N + C_f$, where C_f is a constant depending only on f. By Corollaries 4.3 and 4.5, there are at most

$$O\Big((1 + 2\sqrt{(\log N + C'_f)/(\log|d| + C_f)})^{\operatorname{rank}(E_d)}\Big)$$

rational points P of height $\widehat{h}(P) \le N + C_f$. We proceed as in Proposition 4.12, and conclude that

$$\sum_{0<|d|\le M} \#\{x,y,z \in \mathbb{Z}^3 : |x|,|z| \le N,\ \gcd(x,z)=1,\ dy^2 = f(x,z)\}$$

is at most $O(MN(\log N))^A$. Set $\beta = 1/3$. ∎

4.6. *Homogeneous quintics.* We extract the following result from [Gre].

LEMMA 4.14. *Let $f \in \mathbb{Z}[x,y]$ be a homogeneous irreducible polynomial of degree at most 5. For all $M < N^{\deg f}$, $\varepsilon > 0$,*

$$\sum_{d=1}^{M} \#\{x,y,z \in \mathbb{Z}^3 : |x|,|z| \le N,\ \gcd(x,z)=1,\ dy^2 = f(x,z)\}$$

is at most a constant times $N^{(18-\frac{1}{2}\beta^2)/(10-\beta)+\varepsilon}$, where $\beta = (\log M)/(\log N)$. The implied constant depends only on f and ε.

Proof. By [Gre, Lemmas 5 and 6], where the parameters d and z (in the notation of [Gre]) are set to the values $d = 1$ and $z = N^{(1-\beta/2)/(5/2-\beta/4)}$. ∎

PROPOSITION 4.15. *Let $f \in \mathbb{Z}[x,z]$ be a homogeneous irreducible polynomial of degree 5. Let*

$$\delta(N) = \#\{x,z \in \mathbb{Z}^2 : |x|,|z| \le N,\ \gcd(x,z)=1,\ \exists p > N,\ p^2 \mid P(x,z)\}.$$

Then, for any $\varepsilon > 0$,

$$\delta(N) \ll N^{(5+\sqrt{113})/8+\varepsilon}$$

where the implied constant depends only on f *and* ε.

Proof. Let $A = \max_{|x|,|z|\leq N} f(x,z)$. Clearly $A \ll N^{\deg(f)}$. We can write

$$\delta(N) \leq \sum_{0<|d|\leq M} \#\{x,y,z \in \mathbb{Z}^3 : |x|,|z| \leq N,\ \gcd(x,z)=1,\ dy^2 = f(x,z)\}$$
$$+ \sum_{N<p\leq\sqrt{A/M}} \#\{x,z \in \mathbb{Z}^2 : |x|,|z| \leq N,\ \gcd(x,z)=1,\ p^2 \mid f(x,z)\}.$$

By Lemmas 4.14 and 4.11,

$$\delta(N) \ll N^{(18-\frac{1}{2}\beta^2)/(10-\beta)+\varepsilon} + \frac{1}{\log N}\sqrt{N^{\deg(f)-\beta}},$$

where $\beta = (\log M)/(\log N)$. Set $\beta = (15-\sqrt{113})/4$. ∎

4.7. *Quasiorthogonality, kissing numbers and cubics*

Lemma 4.16 (cf. [GS, Proposition 5]). *Let* $f \in \mathbb{Z}[x]$ *be a cubic polynomial of non-zero discriminant. Let d be a square-free integer. Then, for any two distinct integer points* $P = (x,y) \in \mathbb{Z}^2$, $P' = (x',y') \in \mathbb{Z}^2$ *on the elliptic curve*

$$E_d:\ dy^2 = f(x),$$

we have

$$\widehat{h}(P+P') \leq 3\max(\widehat{h}(P), \widehat{h}(P')) + C_f,$$

where C_f *is a constant depending only on* f.

Proof. Write $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$. Let $P + P' = (x'', y'')$. By the group law,

$$\begin{aligned} x'' &= \frac{d(y_2-y_1)^2}{a_3(x_2-x_1)^2} - \frac{a_2}{a_3} - x_1 - x_2 \\ &= \frac{d(y_2-y_1)^2 - a_2(x_2-x_1)^2 - a_3(x_2-x_1)^2(x_1+x_2)}{a_3(x_2-x_1)^2}. \end{aligned}$$

Clearly $|a_3(x_2-x_1)^2| \leq 4|a_3|\max(|x_1|^2, |x_2|^2)$. Now

$$|d(y_2-y_1)^2| \leq 4|d|\max(y_1^2, y_2^2) = 4\max(|f(x_1)|, |f(x_2)|).$$

Hence

$$|d(y_2-y_1)^2 - a_2(x_2-x_1)^2 - a_3(x_2-x_1)^2(x_1+x_2)| \leq A\max(|x|^3, |x'|^3),$$

where A is a constant depending only on f. Therefore

$$\begin{aligned} h_x(P) &= \log(\max(|\mathrm{num}(x'')|, |\mathrm{den}(x'')|)) \\ &\leq 3\max(\log|x|, \log|x'|) + \log A \leq 3\max(h_x(P), h_x(P')) + \log A. \end{aligned}$$

By Lemma 4.1, the difference $|\widehat{h}-h_x|$ is bounded by a constant independent of d. The statement follows immediately. ■

Consider the elliptic curve

$$E_d:\ dy^2 = f(x).$$

There is a $\mathbb{Z}$-linear map from $E_d(\mathbb{Q})$ to $\mathbb{R}^{\mathrm{rank}(E_d)}$ taking the square of the Euclidean norm back to the canonical height. In other words, any given integer point $P=(x,y)\in E_d$ will be taken to a point $L(P)\in\mathbb{R}^{\mathrm{rank}(E_d)}$ whose Euclidean norm $|L(P)|$ satisfies

$$|L(P)|^2 = \widehat{h}(P) = \log x + O(1),$$

where the implied constant depends only on f. In particular, the set of all integer points $P=(x,y)\in E_d$ with

$$N^{1-\varepsilon}\le x\le N \tag{4.16}$$

will be taken to a set of points $L(P)$ in $\mathbb{R}^{\mathrm{rank}(E_d)}$ with

$$(1-\varepsilon)\log N + O(1) \le |L(P)|^2 \le \log N + O(1).$$

Let $P, P'\in E_d$ be integer points satisfying (4.16). Assume $L(P)\ne L(P')$. By Lemma 4.16,

$$|L(P)+L(P')|^2 = |L(P+P')|^2 \le 3\max(|L(P)|^2, |L(P')|^2) + O(1).$$

Therefore, the inner product $L(P)\cdot L(P')$ satisfies

$$\begin{aligned} L(P)\cdot L(P') &= \frac{1}{2}\left(|L(P)+L(P')|^2 - (|L(P)|^2+|L(P')|^2)\right)\\ &\le \frac{1}{2}\left(3\max(|L(P)|^2,|L(P')|^2)+O(1)-(|L(P)|^2+|L(P')|^2)\right)\\ &\le \frac{1}{2}\left((1+\varepsilon)\log(N)+O(1)\right)\\ &\le \frac{1}{2}\,\frac{(1+\varepsilon)+O((\log N)^{-1})}{(1-\varepsilon)^2}\,|L(P)|\,|L(P')|. \end{aligned}$$

We have proven

LEMMA 4.17. *Let $f\in\mathbb{Z}[x]$ be a cubic polynomial of non-zero discriminant. Let d be a square-free integer. Consider the elliptic curve*

$$E_d:\ dy^2 = f(x).$$

Let S be the set

$$\{(x,y)\in\mathbb{Z}^2 : N^{1-\varepsilon}\le |x|\le N,\ dy^2 = f(x)\}.$$

Let L be a linear map taking $E(\mathbb{Q})$ to $\mathbb{R}^{\mathrm{rank}(E_d)}$ and the square of the Euclidean norm back to the canonical height $\widehat{h}$. Then, for any distinct points

$P, P' \in L(S) \subset \mathbb{R}^{\operatorname{rank}(E_d)}$, the angle θ between P and P' is at least

$$\arccos\left(\frac{1}{2}\,\frac{(1+\varepsilon)+O((\log N)^{-1})}{(1-\varepsilon)^2}\right) = 60^\circ + O(\varepsilon + (\log N)^{-1}),$$

where the implied constant depends only on f.

Let $A(\theta, n)$ be the maximal number of points that can be arranged in $\mathbb{R}^n$ with angular separation no smaller than θ. Kabatyanskiĭ and Levenshteĭn ([KL]; vd. also [CS, (9.6)]) show that, for n large enough,

$$\frac{1}{n}\log_2 A(n,\theta) \leq \frac{1+\sin\theta}{2\sin\theta}\log_2\frac{1+\sin\theta}{2\sin\theta} - \frac{1-\sin\theta}{2\sin\theta}\log_2\frac{1-\sin\theta}{2\sin\theta}. \tag{4.17}$$

Thus we obtain

Corollary 4.18. *Let $f \in \mathbb{Z}[x]$ be a cubic polynomial of non-zero discriminant. Let d be a square-free integer. Consider the elliptic curve*

$$E_d: \; dy^2 = f(x).$$

Let S be the set

$$\{(x,y) \in \mathbb{Z}^2 : N^{1-\varepsilon} \leq |x| \leq N,\, dy^2 = f(x)\}.$$

Then

$$\#S \ll 2^{(\alpha + O(\varepsilon + (\log N)^{-1}))\operatorname{rank}(E_d)},$$

where

$$\alpha = \frac{2+\sqrt{3}}{2\sqrt{3}}\log_2\frac{2+\sqrt{3}}{2\sqrt{3}} - \frac{2-\sqrt{3}}{2\sqrt{3}}\log_2\frac{2-\sqrt{3}}{2\sqrt{3}} = 0.4014\ldots \tag{4.18}$$

and the implied constants depend only on f.

Notice that we are using the fact that the size of the torsion group is bounded.

Proposition 4.19. *Let $f \in \mathbb{Z}[x]$ be an irreducible cubic polynomial. Let*

$$\delta(N) = \#\{1 \leq x \leq N : \exists p > N^{1/2},\, p^2 \mid f(x)\}.$$

Then

$$\delta(N) \ll N(\log N)^{-\beta}, \tag{4.19}$$

where

$$\beta = 1 - \frac{1}{9}\cdot 2^{2\alpha} = 0.8061\ldots$$

if the discriminant of f is a square,

$$\beta = 1 - \frac{1}{6}\cdot 2^{\alpha} - \frac{1}{18}\cdot 2^{2\alpha} = 0.6829\ldots$$

if the discriminant of f is not a square, and α is as in (4.18). *The implied constant in* (4.19) *depends only on f.*

Proof. Let $A = \max_{1\le x\le N} f(x)$. Clearly $A \ll N^3$. We can write

$$\begin{aligned}\delta(N) \le &\sum_{N^{1/2}<p<\sqrt{A/M}} \#\{1\le x\le N : p^2 \mid f(x)\}\\ &+ \#\{1\le x\le N^{1-\varepsilon} : \exists p > N^{1/2},\, p^2\mid f(x)\}\\ &+ \sum_{1\le |d|\le M} \#\{x,y\in\mathbb{Z}^2 : N^{1-\varepsilon}\le x\le N,\, dy^2 = f(x)\}.\end{aligned}$$

Let $M \le N^2$. Then the first term is at most

$$\sum_{N^{1/2}<p<\sqrt{A/M}} 3 \ll \frac{3\sqrt{A/M}}{\log\sqrt{A/M}} \ll \frac{N^{3/2}M^{-1/2}}{\log N}.$$

The second term is clearly no greater than $N^{1-\varepsilon}$. It remains to bound $\sum_{1\le|d|\le M} B(d)$, where

$$B(d) = \#\{x,y\in\mathbb{Z}^2 : N^{1-\varepsilon}\le x\le N,\, dy^2 = f(x)\}.$$

By Lemma 4.8, Corollary 4.18 and the remark before (4.8),

$$B(d) \ll R(\alpha + O(\varepsilon + (\log N)^{-1}), d),$$

where K is as in Lemma 4.8 and α is as in Corollary 4.18 and $R(\alpha, d)$ is as in (4.8). Thanks to (4.14), we can omit the term $O((\log N)^{-1})$ from the exponent. Hence it remains to estimate $S(M) = \sum_{1\le d\le M} R(\alpha + O(\varepsilon + (\log N)^{-1}), d)$. By Lemma 4.10,

$$S(M) \ll \begin{cases} M(\log M)^{\frac{1}{3}2^{2(\alpha+O(\varepsilon))}-1} & \text{if } K/\mathbb{Q} \text{ is Galois,}\\ M(\log M)^{\frac{1}{2}2^{\alpha+O(\varepsilon)}+\frac{1}{6}2^{2(\alpha+O(\varepsilon))}-1} & \text{if } K/\mathbb{Q} \text{ is not Galois.}\end{cases}$$

Set

$$M = \begin{cases} N(\log N)^{-\frac{2}{9}2^{2\alpha}} & \text{if } K/\mathbb{Q} \text{ is Galois,}\\ N(\log N)^{-\frac{1}{3}2^{\alpha}-\frac{1}{9}2^{2\alpha}} & \text{if } K/\mathbb{Q} \text{ is not Galois.}\end{cases}$$

Let $\varepsilon = (\log\log M)^{-1}$. Since $K/\mathbb{Q}$ is Galois if and only if the discriminant of f is a square, the statement follows. ∎

4.8. *Hyperelliptic curves, Mumford's gap and sextics.* We will first need a few lemmas on hyperelliptic curves. See [BK, pp. 718–734] for the analogous statements on elliptic curves. Cf. also [CF, §7.5], and [FPS, Prop. 3]. As is usual, when we speak of the curve $C : y^2 = f(x)$, $\deg(f) \ge 5$, we mean the non-singular projective curve in which the affine curve $y^2 = f(x)$ is contained.

LEMMA 4.20. *Let $f(x) \in K[x]$ be a polynomial of degree 6 defined over a field K of characteristic zero. Let C be the curve $y^2 = f(x)$. Let A_K be the K-algebra $K[x]/f[x]$. Write $A_K = \bigoplus_j K_j$, where each K_j is a finite extension* *of K corresponding to an irreducible factor of K. Define $N_{A_K/K} : A_K \to K$ to be the product of all norms $N_{K_j/K} : K_j \to K$. Let J be the Jacobian of C. Then there is a homomorphism*

$$\mu : J(K) \to A_K^*/K^*(A_K^*)^2$$

whose image is in the kernel of

$$A^*/K^*(A_K^*)^2 \xrightarrow{N_{A_K/K}} K^*/(K^*)^2$$

and whose kernel is generated by $2J(K)$ and at most one element of $J(K)$ not in $2J(K)$. The map μ commutes with field extensions $K \to K'$:

$$\begin{array}{ccc} J(K) & \longrightarrow & A_K^*/K^*(A_K^*)^2 \\ \downarrow & & \downarrow \\ J(K') & \longrightarrow & A_{K'}^*/K'^*(A_{K'}^*)^2 \end{array} \tag{4.20}$$

Proof. See [Ca, p. 30], for the statement on the image and kernel of μ. The commutativity of (4.20) follows from the construction of μ in [Ca, pp. 50–51]. ∎

Given K and $A_K = \bigoplus_j K_j$ as in Lemma 4.20, we speak of the coordinates $(x_j) \in \bigoplus_j K_j$ of a point $x \in A_K$ in the natural fashion.

LEMMA 4.21. *Let $f(x) \in K[x]$ be a polynomial of degree 6 defined over a $\mathfrak{p}$-adic field K whose residue field has odd characteristic. Suppose $C : y^2 = f(x)$ has good reduction. Let μ be as in Lemma 4.20. Let (x_j) be the coordinates of a representative $x \in A_K^*$ of a point $\mu(y) \in A_K^*/K^*(A_K^*)^2$ in the image of μ. Then $v_{K_j}(x_j) \bmod 2$ is independent of j.*

Proof. Let k be the residue field of K, $\widetilde{K}$ the maximal unramified extension of K, and $\bar{k}$ the algebraic closure of k. Let $J_1(\widetilde{K})$ be the kernel of the residue map $J(\widetilde{K}) \to J(\bar{k})$. We have an exact sequence

$$0 \to J_1(\widetilde{K}) \to J(\widetilde{K}) \to J(\bar{k}) \to 0,$$

from which we obtain

$$J_1(\widetilde{K})/2J_1(\widetilde{K}) \to J(\widetilde{K})/2J(\widetilde{K}) \to J(\bar{k})/2J(\bar{k}) \to 0.$$

Since $\bar{k}$ is algebraically closed, the group $J(\bar{k})/2J(\bar{k})$ is trivial. Since $J_1(\widetilde{K})$ is isomorphic to a formal group over k ([CF, (7.3.5)]) and the characteristic of k is not 2, the group $J(\widetilde{K})/2J(\widetilde{K})$ is trivial as well. Hence $J(\widetilde{K})/2J(\widetilde{K})$ is trivial.

By virtue of the commutative diagram

$$\begin{array}{ccc} J(K)/2J(K) & \xrightarrow{\mu} & A_K^*/K^*(A_K^*)^2 \\ \downarrow & & \\ J(\widetilde{K})/2J(\widetilde{K}) = \{e\} & \xrightarrow{\mu} & A_{\widetilde{K}}^*/\widetilde{K}^*(A_{\widetilde{K}}^*)^2 \end{array}$$

the image of $\mu(J(K)/2J(K))$ lies in $A_{\widetilde{K}}^* \cap \widetilde{K}^*(A_{\widetilde{K}}^*)^2$. Since, for every index j, the extensions $\widetilde{K}_j/K_j$ and $\widetilde{K}_j/\widetilde{K}$ are unramified, we can write, for any $r \in \widetilde{K}^*$, $s \in A_{\widetilde{K}}^*$ with $rs^2 \in A_{\widetilde{K}}^*$,

$$v_{K_j}(rs^2) = v_{\widetilde{K}_j}(rs^2) = v_{\widetilde{K}_j}(r) + 2v_{\widetilde{K}_j}(s) = v_{\widetilde{K}}(r) + 2v_{\widetilde{K}_j}(s).$$

The statement follows. ∎

PROPOSITION 4.22. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 6. Choose a root x_0 of $f(x) = 0$. Let $L = \mathbb{Q}(x_0)$. For every square-free integer d, let C_d be the hyperelliptic curve $dy^2 = f(x)$. Then*

$$\operatorname{rank}(C_d) \leq \kappa_f + \sum_{p|d} (n_p - m_p),$$

where

$$n_p = \text{number of primes of } L \text{ above } p,$$

$$m_p = \begin{cases} 1 & \text{if all primes above } p \text{ are of even inertia degree,} \\ 2 & \text{otherwise,} \end{cases}$$

and κ_f is a constant depending only on f.

Proof. We can identify L with the algebra $A_{\mathbb{Q}}$ from Lemmas 4.20, 4.21; notice that L and $A_{\mathbb{Q}}$ are independent of the twist d. Consider the exact sequence

$$0 \to H \to A_{\mathbb{Q}}^*/\mathbb{Q}^*(A_{\mathbb{Q}}^*)^2 \to \prod_{\nu} (A_{\mathbb{Q}_\nu}^*/\mathbb{Q}_\nu^*(A_{\mathbb{Q}_\nu}^*)^2)/U_{A_{K_\nu}},$$

where $U_{A_{K_\nu}}$ is $V_{A_{K_\nu}} \mathbb{Q}_\nu^*(A_{\mathbb{Q}_\nu}^*)^2$, $V_{A_{K_\nu}}$ is the subgroup of $A_{\mathbb{Q}_\nu}^*$ consisting of the elements $x \in A_{\mathbb{Q}_\nu}^*$ all of whose coordinates are units, and H is the subgroup of $L^*/\mathbb{Q}^*(L^*)^2 = A_{\mathbb{Q}}^*/\mathbb{Q}^*(A_{\mathbb{Q}}^*)^2$ consisting of such cosets as are represented by elements $x \in L^*$ with $(x) = r\mathfrak{s}^2$ for some $r \in \mathbb{Q}$, $\mathfrak{s} \in I_L$. Clearly

$$\operatorname{rank}(H) \leq 5 + \operatorname{rank}(h_L/h_L^2),$$

where h_L is the class group of L. Hence the rank of the kernel of the composition

$$c : J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q}) \xrightarrow{\mu} A_{\mathbb{Q}}^*/\mathbb{Q}^*(A_{\mathbb{Q}}^*)^2 \to \prod_{\nu} (A_{\mathbb{Q}_\nu}^*/\mathbb{Q}_\nu^*(A_{\mathbb{Q}_\nu}^*)^2)/U_{A_{\mathbb{Q}_\nu}}$$

is at most $6+\mathrm{rank}(h_L/h_L^2)$. We have a commutative diagram

$$\begin{array}{ccc} J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q}) & \xrightarrow{c} & \prod_\nu (A^*_{\mathbb{Q}_\nu}/\mathbb{Q}^*_\nu(A^*_{\mathbb{Q}_\nu})^2)/U_{A_{\mathbb{Q}_\nu}} \\ \downarrow & & \downarrow \\ J_{C_d}(\mathbb{Q}_\nu)/2J_{C_d}(\mathbb{Q}_\nu) & \xrightarrow{\mu} & (A^*_{\mathbb{Q}_\nu}/\mathbb{Q}^*_\nu(A^*_{\mathbb{Q}_\nu})^2)/U_{A_{\mathbb{Q}_\nu}} \end{array}$$

By Lemma 4.21, the bottom row has trivial image when $\nu \neq 2,\infty$ and C_d has good reduction at ν. Thus

$$\begin{aligned} \mathrm{rank}(J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q})) &\leq 6+\mathrm{rank}(h_L/h_L^2) \\ &+ \sum_{\substack{\nu=\infty,2 \text{ or} \\ L \text{ ramifies at } \nu \text{ or} \\ C_1 \text{ has bad reduction at } \nu}} \mathrm{rank}((A^*_{\mathbb{Q}_\nu}/\mathbb{Q}^*_\nu(A^*_{\mathbb{Q}_\nu})^2)/U_{A_{\mathbb{Q}_\nu}}) \\ &+ \sum_{\substack{p\mid d \\ p \text{ unramified in } L/\mathbb{Q}}} \mathrm{rank}(\mu(J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q}))). \end{aligned}$$

By Lemma 4.20, $\mu(J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q}))$ is contained in the intersection of $(A^*_{\mathbb{Q}_\nu}/\mathbb{Q}^*_\nu(A^*_{\mathbb{Q}_\nu})^2)/U_{A_{\mathbb{Q}_\nu}}$ with the kernel of $N_{A_\mathbb{Q}/\mathbb{Q}}$. Hence the image of

$$\mu(J_{C_d}(\mathbb{Q}_\nu)/2J_{C_d}(\mathbb{Q}_\nu))$$

under the natural injection

$$(A^*_{\mathbb{Q}_\nu}/\mathbb{Q}^*_\nu(A^*_{\mathbb{Q}_\nu})^2)/U_{A_{\mathbb{Q}_\nu}} \to \Big(\bigoplus_{\mathfrak{p}\mid p} \mathbb{Z}/2\mathbb{Z}\Big)/(1,\ldots,1)$$

consists of cosets $(x_\mathfrak{p})_{\mathfrak{p}\mid p} \in \bigoplus_{\mathfrak{p}\mid p}\mathbb{Z}/2\mathbb{Z}$ with $\sum_{\mathfrak{p}\mid p} f_\mathfrak{p} x_\mathfrak{p}$ even. There are $2^{n_p-m_p}$ such cosets, where n_p and m_p are as in the statement of the present lemma. Therefore

$$\begin{aligned} &\mathrm{rank}(J_{C_d}(\mathbb{Q})) \leq \mathrm{rank}(J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q})) \\ &\quad \leq 6+\mathrm{rank}(h_L/h_L^2) \\ &\quad + \sum_{\substack{\nu=\infty,2 \text{ or} \\ L \text{ ramifies at } \nu \text{ or} \\ C_1 \text{ has bad reduction at } \nu}} \mathrm{rank}((A^*_{\mathbb{Q}_\nu}/\mathbb{Q}^*_\nu(A^*_{\mathbb{Q}_\nu})^2)/U_{A_{\mathbb{Q}_\nu}}) + \sum_{p\mid d}(n_p-m_p). \quad \blacksquare \end{aligned}$$

4.9. *More averages of divisor functions.* The following lemma is an analytical variant on Chebotarev's theorem. We denote the conjugacy class of a map $\phi \in \mathrm{Gal}(K/\mathbb{Q})$ by $\langle\phi\rangle$.

LEMMA 4.23. *Let $K/\mathbb{Q}$ be a Galois number field. Let $\langle\gamma\rangle$ be a conjugacy class in $G = \mathrm{Gal}(K/\mathbb{Q})$. Then, for $\Re(s) > 1$,*

$$\prod_{\substack{p \\ \mathrm{Frob}_p=\langle\gamma\rangle}} (1-p^{-s})^{-1} = L_0(s)\prod_\chi L_\chi(s)^{\overline{\chi(\gamma)}\#\langle\gamma\rangle/\#G},$$

where

- L_0 *is holomorphic and bounded on* $\{s \in \mathbb{C} : \Re(s) \geq 1/2 + \varepsilon\}$,
- *the product* $\prod_\chi$ *is taken over all characters* χ *of* G,
- L_χ *is the Artin* L*-function corresponding to the character* χ.

Proof. For every character χ of G, the L-function L_χ is of the form

$$L_0(s) \prod_p (1 - \chi(\mathrm{Frob}_p) p^{-s})^{-1},$$

where $L_0(s)$ is some function holomorphic and bounded for $\Re(s) \geq 1/2 + \varepsilon$. By the orthogonality of the characters of G, we see that $\sum_\chi \chi(\mathrm{Frob}_p)\overline{\chi(\gamma)}$ is $|G|$ for $\langle \mathrm{Frob}_p \rangle = \langle \gamma \rangle$, and 0 otherwise. ∎

COROLLARY 4.24. *Let* $K/\mathbb{Q}$ *be a Galois number field. Let* $g : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}$ *be given. Then*

$$\sum_{d \leq X} \prod_{p|d} g(\mathrm{Frob}_p) = C_{K,g} X (\log X)^{-1 + (\#G)^{-1} \sum_{\gamma \in G} g(\gamma)},$$

where $G = \mathrm{Gal}(K/\mathbb{Q})$, $C_{K,g}$ *is a positive constant depending only on* K *and* $g(\gamma)$ *for all* $\gamma \in G$, *and the dependence of* $C_{K,g}$ *on* $g(\gamma)$ *is continuous for every* $\gamma \in G$.

Proof. Clearly

$$\sum_n \prod_{p|d} g(\mathrm{Frob}_p) n^{-s} = \prod_{\langle\gamma\rangle} \prod_{\substack{p \\ \mathrm{Frob}_p = \langle\gamma\rangle}} (1 + g(\gamma)p^{-s} + g(\gamma)p^{-2s} + \cdots),$$

where the product $\prod_{\langle\gamma\rangle}$ is taken over all conjugacy classes $\langle\gamma\rangle$ in G. By Lemma 4.23,

$$\prod_{\substack{p \\ \mathrm{Frob}_p = \langle\gamma\rangle}} (1 + g(\gamma)p^{-s} + g(\gamma)p^{-2s} + \cdots) = L_0(s) \prod_\chi L_\chi(s)^{g(\gamma)\overline{\chi(\gamma)}\#\langle\gamma\rangle/\#G},$$

where L_0 is holomorphic and bounded on $\Re(s) \geq 1/2 + \varepsilon$. Hence

$$\sum_n \prod_{p|d} g(\mathrm{Frob}_p) n^{-s} = L_0(s) \prod_\chi L_\chi(s)^{\sum_{\langle g\rangle} g(\gamma)\overline{\chi(\gamma)}\#\langle\gamma\rangle/\#G}.$$

Artin L-functions associated to non-principal characters χ are holomorphic and bounded on a neighborhood of $s = 1$. By a Tauberian theorem (e.g., [PT, Main Th.]), the statement follows. ∎

Let $K/\mathbb{Q}$ be a number field; let $K'/\mathbb{Q}$ be its Galois closure. We can see $\mathrm{Gal}(K'/\mathbb{Q})$ as a transitive permutation group on $\{1, \ldots, \deg(K/\mathbb{Q})\}$. Since every permutation of $\{1, \ldots, n\}$ is a product of disjoint cycles, we may speak of the cycles of a map $\gamma \in \mathrm{Gal}(K'/\mathbb{Q})$. We write $G_1(K'/\mathbb{Q})$ for the set of all $\gamma \in \mathrm{Gal}(K'/\mathbb{Q})$ fixing at least one point in $\{1, \ldots, \deg(K, \mathbb{Q})\}$.

Corollary 4.25. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 6. For every square-free integer d, let C_d be the hyperelliptic curve $dy^2 = f(x)$. Let α be a positive real number. Write K' for the splitting field of f. Choose a root x_0 of $f(x) = 0$. Let $K = \mathbb{Q}(x_0)$. Let $R(\alpha, d) = 2^{\alpha \operatorname{rank}(C_d)}$ if no $p \mid d$ is unsplit in $K/\mathbb{Q}$. Let $R(\alpha, d) = 0$ otherwise. Then*

$$\sum_{d \leq X} R(\alpha, d) \ll X (\log X)^{\delta - 1}, \tag{4.21}$$

where

$$\delta = \frac{1}{\operatorname{Gal}(K'/\mathbb{Q})} \sum_{\gamma \in G_1(K'/\mathbb{Q})} 2^{\alpha(n_\gamma - 2)},$$

n_γ is the number of cycles of γ, and the implied constant in (4.21) *depends only on K and α; the dependence on α is continuous.*

Proof. Immediate from Proposition 4.22 and Corollary 4.24. ■

Table 1. Galois groups and corresponding averages

$\operatorname{Gal}(K'/\mathbb{Q})$	δ	for $\alpha = 0.4014\ldots$
$C(6)$	$\frac{1}{6} 2^{4\alpha}$	$0.5072\ldots$
$D_6(6)$	$\frac{1}{6} 2^{4\alpha}$	$0.5072\ldots$
$D(6)$	$\frac{1}{4} 2^{2\alpha} + \frac{1}{12} 2^{4\alpha}$	$0.6897\ldots$
$A_4(6)$	$\frac{1}{4} 2^{2\alpha} + \frac{1}{12} 2^{4\alpha}$	$0.6897\ldots$
$F_{18}(6)$	$\frac{2}{9} 2^{2\alpha} + \frac{1}{18} 2^{4\alpha}$	$0.5567\ldots$
$2A_4(6)$	$\frac{1}{8} 2^{2\alpha} + \frac{1}{8} 2^{3\alpha} + \frac{1}{24} 2^{4\alpha}$	$0.6328\ldots$
$S_4(6d)$	$\frac{3}{8} 2^{2\alpha} + \frac{1}{24} 2^{4\alpha}$	$0.7809\ldots$
$S_4(6c)$	$\frac{1}{4} 2^{\alpha} + \frac{1}{8} 2^{2\alpha} + \frac{1}{24} 2^{4\alpha}$	$0.6750\ldots$
$F_{18}(6):2$	$\frac{13}{36} 2^{2\alpha} + \frac{1}{36} 2^{4\alpha}$	$0.7145\ldots$
$F_{36}(6)$	$\frac{13}{36} 2^{2\alpha} + \frac{1}{36} 2^{4\alpha}$	$0.7145\ldots$
$2S_4(6)$	$\frac{1}{8} 2^{\alpha} + \frac{3}{16} 2^{2\alpha} + \frac{1}{16} 2^{3\alpha} + \frac{1}{48} 2^{4\alpha}$	$0.6996\ldots$
$L(6)$	$\frac{2}{5} + \frac{1}{4} 2^{2\alpha} + \frac{1}{60} 2^{4\alpha}$	$0.8868\ldots$
$F_{36}(6):2$	$\frac{1}{6} 2^{\alpha} + \frac{13}{72} 2^{2\alpha} + \frac{1}{12} 2^{3\alpha} + \frac{1}{72} 2^{4\alpha}$	$0.7693\ldots$
$L(6):2$	$\frac{1}{5} + \frac{1}{4} 2^{\alpha} + \frac{1}{8} 2^{2\alpha} + \frac{1}{120} 2^{4\alpha}$	$0.7736\ldots$
A_6	$\frac{2}{5} + \frac{17}{72} 2^{2\alpha} + \frac{1}{360} 2^{4\alpha}$	$0.8203\ldots$
S_6	$\frac{1}{5} + \frac{7}{24} 2^{\alpha} + \frac{17}{144} 2^{2\alpha} + \frac{1}{48} 2^{3\alpha} + \frac{1}{720} 2^{4\alpha}$	$0.8434\ldots$

Table 1 gives the value of δ in terms of α and $\operatorname{Gal}(K'/\mathbb{Q})$. The numerical value of δ for $\alpha = 0.4014\ldots$ is given in the rightmost column. The table was computed by means of the finite-group package GAP [GAP4] running on a GNU/Linux box. The sixteen transitive permutation groups on $\{1, \ldots, 6\}$ have been labelled as in [CHM].

4.10. *Rational points and ranks of Jacobians*

LEMMA 4.26. *Let K be a number field. Let $f \in K[x]$ be an irreducible polynomial of degree 6. Let C be the curve $y^2 = f(x)$. For every $d \in K^*$, let C_d be the curve $dy^2 = f(x)$. Let c be a divisor of the Jacobian J_C of C. Then the image of $C_d(K)$ under the composition*

$$\phi_{d,c} : C_d(K) \xrightarrow{(x,y)\mapsto(x,y\sqrt{d})} C \xrightarrow{P\mapsto \mathrm{Cl}(P)-c} J_C \tag{4.22}$$

generates an abelian group of rank at most $\mathrm{rank}(J_{C_d}(K)) + 1$.

Proof. We have a commutative diagram

$$\begin{array}{ccc} C_d(K) & \xrightarrow{\mu} & C \\ \downarrow & & \downarrow \\ J_{C_d} & \xrightarrow{\sim} & J_C \end{array}$$

where the equivalence at the bottom is induced by $t_d : (x,y) \mapsto (x, y\sqrt{d})$, and the map on the left is given by $P \to \mathrm{Cl}(P) - t_d^* c$. If $C_d(K)$ is empty, we have nothing to prove. Assume that $C_d(K)$ has at least one element, and call it P_0. The image of

$$C_d(K) \xrightarrow{P\mapsto \mathrm{Cl}(P)-\mathrm{Cl}(P_0)} J_{C_d}$$

is an abelian group of rank no greater than $\mathrm{rank}(J_{C_d(K)})$. Hence, the corresponding subgroup of J_C under the isomorphism $J_{C_d} \equiv J_C$ has rank at most $\mathrm{rank}(J_{C_d(K)})$ as well. This subgroup is the image of $C_d(K)$ under the composition

$$C_d(K) \xrightarrow{(x,y)\mapsto(x,y\sqrt{d})} C \xrightarrow{P\mapsto \mathrm{Cl}(P)-(t_d^{-1})^*(\mathrm{Cl}(P_0))} J_C.$$

If we displace the subgroup by $(t_d^{-1})^*(\mathrm{Cl}(P_0)) - c$, we obtain $\phi_{d,c}(C_d(K))$. The statement follows immediately. ∎

PROPOSITION 4.27 (Mumford). *Let K be a number field. Let C be a complete non-singular curve over K with genus $g \geq 2$. Let J_C be the Jacobian of C. Let h_δ be the height function on $J \times J$ induced by the theta divisor*; *let $P \to \mathrm{Cl}(P) - c_0$ be a normalized embedding of C in J, where c_0 is an appropriately chosen divisor of C.* (See [La, p. 113 and p. 120].) *Define*

$$\langle P_1, P_2 \rangle = -h_\delta(P_1, P_2), \qquad |P| = \sqrt{\langle P, P \rangle}. \tag{4.23}$$

Then, for any $P_1, P_2 \in C(\overline{K})$, $P_1 \neq P_2$,

$$2g\langle P_1, P_2 \rangle \leq |P_1|^2 + |P_2|^2 + O(1).$$

Notice moreover that

$$\langle P, P \rangle = 2g h_{c_0}(P) + O(1)$$

for any point P of C. The implied constants depend only on C and on the choice of c_0.

Proof. See [La, Thm. 5.10 and Thm. 5.11]. (The original formulation in [Mu] is restricted to rational points.) ∎

LEMMA 4.28. *Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 6. For every square-free integer d, let C_d be the curve $dy^2 = f(x)$. Let c_0 be as in Proposition 4.27 and let ϕ_{d,c_0} be as in (4.22). Then there is a constant κ_f such that, if d is a square-free integer larger than κ_f, there are at most 8 points P in $C_d(\mathbb{Q})$ for which $\phi_{d,c_0}(P)$ is torsion.*

Proof. Consider the divisor h_y on $C = C_1$. It is clear that $P = (x, y\sqrt{d})$ lies on C, and that $h_y(P) = y\sqrt{d} + O_f(1)$. By [La, Ch. 4, Cor. 3.5],

$$(1-\varepsilon)\kappa_0 h_{c_0}(P) - \kappa_\varepsilon \leq h_y((x, y\sqrt{d})) \leq (1+\varepsilon)\kappa_0 h_{c_0}(P) + \kappa_\varepsilon$$

for every $\varepsilon > 0$ and some κ_0, κ_ε, where κ_ε depends only on f and ε. By [La, Thm. 5.10], $h_{c_0}(P) = \frac{1}{4}|P|^2 + O(1)$, where $|P|$ is as in (4.23). Suppose $\phi_{d,c_0}(P)$ is torsion. Then $|P| = 0$. We deduce that $h_{c_0}(P)$ is bounded, and hence so is $h_y(P)$; yet, by Lemma 4.2, we know that either $h_y(P) \geq \frac{3}{8}\log|d| + O_f(1)$, or $y = 0$, or $(x, y\sqrt{d})$ is one of the two points of C at infinity. If d is large enough, we can conclude that either $y = 0$ or $(x, y\sqrt{d}) = \pm\infty$. There are six solutions to the former equation and two to the latter. ∎

As is usual, we speak of the rank of a curve C when we mean the rank of its Jacobian. Thus $\mathrm{rank}(C)$ and $\mathrm{rank}(J_C)$ are the same.

PROPOSITION 4.29. *Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 6. For every square-free integer d, let C_d be the curve $dy^2 = f(x)$. For $0 < \varepsilon < 1/2$, let*

$$S = \{(x, y) \in C_d(\mathbb{Q}) : (1-\varepsilon)x_0 \leq H(x) \leq (1+\varepsilon)x_0\}.$$

Then

$$\#S \ll_\varepsilon 2^{(\alpha + O_\varepsilon(x_0^{-2}))\,\mathrm{rank}(C_d(K))},$$

where α is as in (4.18) and the implied constants in $\ll$ and $O_\varepsilon(x_0^{-2})$ depend only on f and ε.

Proof. Let $C = C_1$. Let c_0 be as in Proposition 4.27, ϕ_{d,c_0} as in (4.22). By Lemma 4.26, all points of $\phi_{d,c_0}(C_d(\mathbb{Q}))$ lie on an abelian subgroup of J_C of rank at most $\mathrm{rank}(J_{C_d}(K)) + 1$. The function

$$\langle P_1, P_2\rangle = -h_\delta : J \times J \to \mathbb{R}$$

in Proposition 4.27 is a positive, symmetric quadratic form. We have $\langle P, P\rangle = 0$ if and only if P is torsion. Hence there is a map

$$\iota : \phi_{d,c_0}(C_d(\mathbb{Q})) \to \mathbb{R}^{\mathrm{rank}(J_{C_d}(K))+1}$$

with torsion kernel such that the inner product in $\mathbb{R}^{\operatorname{rank}(J_{C_d}(K))+1}$ is taken back to the inner product $\langle\cdot,\cdot\rangle$ in J. By Lemma 4.28, there are at most 8 points P in $C_d(\mathbb{Q})$ such that $\phi_{d,c_0}(P)$ is torsion. Thus the kernel of ι has cardinality at most 8, and we can focus on determining the cardinality of $\iota(\phi_{d,c_0}(S))$.

Let $P=(x,y)\in S$. By [La, Cor. IV.3.5 and Thm. V.5.10],

$$(1-\varepsilon)^2\kappa_0 x_0-\kappa_\varepsilon\le|\phi_{d,c_0}(P)|^2\le(1+\varepsilon)^2\kappa_0x_0+\kappa_\varepsilon$$

for some κ_0, κ_ε, the latter depending on ε. For any $P_1,P_2\in C_d(\mathbb{Q})$, $P_1\ne P_2$, we see by Proposition 4.27 that

$$\langle\phi_{d,c_0}(P_1),\phi_{d,c_0}(P_2)\rangle\le\frac{|\phi_{d,c_0}(P_1)|^2+|\phi_{d,c_0}(P_2)|^2}{4}+O(1).$$

Hence, for $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)$ in S, $P_1\ne P_2$,

$$\begin{aligned}\frac{\langle\iota(\phi_{d,c_0}(P_1)),\iota(\phi_{d,c_0}(P_2))\rangle}{|\iota(\phi_{d,c_0}(P_1))|\,|\iota(\phi_{d,c_0}(P_2))|}&=\frac{\langle\phi_{d,c_0}(P_1),\phi_{d,c_0}(P_2)\rangle}{|\phi_{d,c_0}(P_1)|\,|\phi_{d,c_0}(P_2)|}\\&\le\frac{|\phi_{d,c_0}(P_1)|/|\phi_{d,c_0}(P_2)|+|\phi_{d,c_0}(P_2)|/|\phi_{d,c_0}(P_1)|+O(x_0^{-2})}{4}\\&\le\frac{(1-\varepsilon)^2/(1+\varepsilon)^2+(1+\varepsilon)^2/(1-\varepsilon)^2+O_\varepsilon(x_0^{-2})}{4}\\&=\frac{(1+6\varepsilon^2+\varepsilon^4)/(1-\varepsilon^2)^2}{2}+O_\varepsilon(x_0^{-2}).\end{aligned}$$

We are in the same situation as in Subsection 4.7: we have to bound the number of points that can lie in $\mathbb{R}^n$ with an angle of at least $60^\circ-\varepsilon$ between any two of them. As before, we can apply (4.18). We obtain

$$\#\iota(S)\ll 2^{(\alpha+O(\varepsilon^2)+O_\varepsilon(x_0^{-2}))(\operatorname{rank}(J_{C_d}(K))+1)},$$

from which the statement immediately follows. ∎

COROLLARY 4.30. *Let $f(x,y)\in\mathbb{Z}[x,y]$ be an irreducible homogeneous polynomial of degree* 6. *Let d be a square-free integer. Consider the curve $C_d: dy^2=f(x,1)$. Let S be the set*

$$\{(x,y,z)\in\mathbb{Z}^3: N^{1-\varepsilon}\le|x|,|z|\le N^{1+\varepsilon},\ dy^2=f(x,z)\}.$$

Then

$$\#S\ll_\varepsilon 2^{(\alpha+O_\varepsilon((\log N)^{-2}))\operatorname{rank}(C_d)},$$

where α is as in (4.18) *and the implied constants in $\ll$ and $O_\varepsilon(x_0^{-2})$ depend only on f and ε.*

Proof. Immediate from Proposition 4.29. ∎

4.11. *The square-free sieve for homogeneous sextics*

PROPOSITION 4.31. *Let $f \in \mathbb{Z}[x,z]$ be an irreducible homogeneous polynomial of degree 6. Let*

$$\delta(N) = \#\{-N \le x, z \le N : \gcd(x,z) = 1,\ \exists p > N^{1/2},\ p^2 \mid f(x,z)\}.$$

Then, for every $\varepsilon > 0$,

$$\delta(N) \ll X(\log X)^{-\beta+\varepsilon}, \tag{4.24}$$

where β is given in Table 2 in terms of the Galois group of the splitting field of $f(x,1) = 0$. The implied constant depends only on f and ε.

Table 2. Square-free sieve for sextics: exponents

Gal	β	Gal	β
$C(6)$	$0.8309\ldots$	$D_6(6)$	$0.8309\ldots$
$D(6)$	$0.7700\ldots$	$A_4(6)$	$0.7700\ldots$
$F_{18}(6)$	$0.8144\ldots$	$2A_4(6)$	$0.7890\ldots$
$S_4(6d)$	$0.7396\ldots$	$S_4(6c)$	$0.7749\ldots$
$F_{18}(6):2$	$0.7618\ldots$	$F_{36}(6)$	$0.7618\ldots$
$2S_4(6)$	$0.7667\ldots$	$L(6)$	$0.7043\ldots$
$F_{36}(6):2$	$0.7435\ldots$	$L(6):2$	$0.7421\ldots$
A_6	$0.7265\ldots$	S_6	$0.7188\ldots$

Proof. Let $A = \max_{1\le x,z\le N} f(x,z)$. Clearly $A \ll N^6$. We can write

$$\begin{aligned}\delta(N) \le &\sum_{N^{1/2}<p<\sqrt{A/M}} \#\{-N \le x,z \le N : p^2 \mid f(x,z)\}\\ &+ \#\{-N^{1-\varepsilon} \le x,z \le N^{1-\varepsilon} : \gcd(x,z)=1,\ \exists p > N^{1/2},\ p^2 \mid f(x,z)\}\\ &+ \sum_{\substack{1\le|d|\le M\\ d\,\text{square-free}}} \#\{x,y,z \in \mathbb{Z}^3 : N^{1-\varepsilon} \le \max(|x|,|z|) \le N,\ dy^2 = f(x,z)\}.\end{aligned}$$

Let $M \le N^2$. By Lemma 4.11, the first term is at most

$$\sum_{N^{1/2}<p<\sqrt{A/M}} 3 \ll \frac{3\sqrt{A/M}}{\log\sqrt{A/M}} \ll \frac{N^3 M^{-1/2}}{\log N}.$$

The second term is clearly no greater than $N^{2-\varepsilon}$. It remains to bound

$$\sum_{\substack{1\le|d|\le M\\ d\,\text{square-free}}} B(d),$$

where

$$B(d) = \#\{x,y,z \in \mathbb{Z}^3 : N^{1-\varepsilon} \le \max(|x|,|z|) \le N,\ dy^2 = f(x,z)\}.$$

By Corollary 4.30,

$$B(d) \ll 2^{(\alpha+O(\varepsilon^2)+O((\log N)^{-2}))\,\mathrm{rank}(C_d)}.$$

By (4.14) and Proposition 4.22, we can omit the term $O((\log N)^{-2})$. Notice also that we can treat d negative just as we do d positive, by working with $-f(x,z)$ instead of $f(x,z)$. Hence it is left to estimate

$$S(M) = \sum_{\substack{1\le d\le M\\ d\,\text{square-free}}} 2^{(\alpha+O(\varepsilon^2))\,\mathrm{rank}(C_d)}.$$

Corollary 4.25 gives us $S(M) \ll M(\log M)^{\delta-1+O(\varepsilon^2)}$, where δ is as in Table 2. Set $M = N^2(\log N)^{-\frac{2}{3}\delta}$. Then

$$S(M) \ll N^2(\log N)^{\frac{1}{3}\delta-1+O(\varepsilon^2)}, \qquad \frac{N^3M^{-1/2}}{\log N} \ll N^2(\log N)^{\frac{1}{3}\delta-1+O(\varepsilon^2)}. \ \blacksquare$$

5. Square-free values of polynomials. We can now state our main unconditional results.

THEOREM 5.1. *Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of degree* 3. *Then the number of positive integers $x \le N$ for which $f(x)$ is square-free is given by*

$$N\prod_p \left(1-\frac{\ell(p^2)}{p^2}\right) + O(N(\log N)^{-\beta}), \tag{5.1}$$

where

$$\beta = \begin{cases} 0.8061\ldots & \text{if the discriminant of } f \text{ is a square},\\ 0.6829\ldots & \text{if the discriminant of } f \text{ is not a square},\end{cases}$$
$$\ell(m) = \#\{x \in \mathbb{Z}/m : f(x) \equiv 0 \bmod m\}.$$

The implied constant in (5.1) *depends only on f.*

Proof. By Propositions 3.4 and 4.19. ■

THEOREM 5.2. *Let $f \in \mathbb{Z}[x,y]$ be a homogeneous polynomial of degree no greater than* 6. *Then the number of integer pairs $(x,y) \in \mathbb{Z}^2 \cap [-N,N]^2$ for which $f(x,y)$ is square-free is given by*

$$4N^2\prod_p \left(1-\frac{\ell_2(p^2)}{p^4}\right) + \begin{cases} O(N^{4/3}(\log N)) & \text{if } \deg_{\mathrm{irr}}(f) \le 4,\\ O(N^{(5+\sqrt{113})/8+\varepsilon}) & \text{if } \deg_{\mathrm{irr}}(f) = 5,\\ O(N^2(\log N)^{-\beta+\varepsilon}) & \text{if } \deg_{\mathrm{irr}}(f) = 6,\end{cases}$$

where ε is an arbitrarily small positive number, β is given in Table 2 *in terms of the Galois group of the splitting field of $f(x,1) = 0$, A depends only on f, the implied constant depends only on f and ε,* $\deg_{\mathrm{irr}}$ *denotes the degree of the irreducible factor of f of largest degree, and*

$$\ell_2(m) = \#\{(x,y) \in (\mathbb{Z}/m)^2 : f(x,y) \equiv 0 \bmod m\}.$$

Proof. By Propositions 3.5, 4.13, 4.12, 4.15 and 4.31. In the case of $\deg f = 1$ and $\deg f = 2$, we reset $M = CN^2$ within Proposition 3.5, where C is any constant such that $|f(x, y)| \leq CN^2$ for all $1 \leq x, y \leq N$. ∎

In the same way as above, we can obtain unconditional results from the propositions in Subsection 3.4 by applying Propositions 4.19, 4.13, 4.12, 4.15 and 4.31.

6. Previous work and work to do. The best bounds known before now are listed in the first table of the introduction. The case $\deg_{\mathrm{irr}}(P(x)) = 2$ was dealt with by Estermann [Es], the case $\deg_{\mathrm{irr}}(P(x)) = 3$ by Hooley [Hoo, Ch. IV]. All entries for $P(x, y)$ homogeneous, $3 \leq \deg_{\mathrm{irr}}(P(x)) \leq 6$, are due to Greaves [Gre]. The bound given in the main theorem of [Gre] for $\deg_{\mathrm{irr}} = 6$ is actually $N^2/(\log N)^{1/3}$, rather than $N^2/(\log N)^{1/2}$. Ramsay ([Ra], 1991) showed that a slight amendment is sufficient to improve the exponent from $(\log N)^{1/3}$ to $(\log N)^{1/2}$. In our formulation, it is enough to substitute Lemma A.5 for [Gre, Lemma 1], within the proof of [Gre, Lemma 2].

Most of the results in the present paper should carry over fairly readily to polynomials over number fields. The estimates in §4, coming from Diophantine geometry, can be generalized at least as easily as bounds coming from sieves. However, we have stated the final results only over $\mathbb{Q}$, except for the cases in which a general treatment required little or no additional space. The main reason for this limitation is that we do not know a priori what kind of generalization is desirable. Given a polynomial $P \in \mathcal{O}_K[x]$, should we examine only its values for $x \in \mathbb{Z}$, or should we let x range over all of $\mathcal{O}_K$? In the latter case, how do we order $\mathcal{O}_K$? A simple ordering by norm will not do, as there are infinitely many elements of $\mathcal{O}_K$ of norm below any given $c > 1$, unless K is imaginary quadratic. One may choose a basis of $\mathcal{O}_K$ and use this basis to inject a box $\{1, \ldots, N\}^{\deg K}$ into $\mathcal{O}_K$, but this procedure is neither canonical nor necessarily natural. It is probably best to wait to see what will be demanded by applications, and to hope that abstract statements such as Proposition 3.2 and Corollary 3.3 will accommodate the required change in the objects of study.

Acknowledgments. I am indebted to my advisor, Henryk Iwaniec, for his guidance. Thanks are due as well to Jordan Ellenberg and Joseph Silverman, for their advice, and to Keith Ramsay, for our discussions on his unpublished work.

Appendix A. Lattices and solutions. We write $\operatorname{Disc} P$ for the discriminant of a polynomial $P \in \mathcal{O}_K[x]$. If P is square-free, then $\operatorname{Disc} P$ is a non-zero element of $\mathcal{O}_K$, and

$$\gcd(P(x), P'(x)) \mid \operatorname{Disc} P$$

for every $x \in \mathcal{O}_K$.

LEMMA A.1. *Let K be a $\mathfrak{p}$-adic field. Let $P \in \mathcal{O}_K[x]$ be a square-free polynomial. Then*

$$P(x) \equiv 0 \bmod \mathfrak{p}^n$$

has at most $\max(|\operatorname{Disc} P|_{\mathfrak{p}}^{-1} \deg P, |\operatorname{Disc} P|_{\mathfrak{p}}^{-3})$ *roots in* $\mathcal{O}_K/\mathfrak{p}^n$.

Proof. Let π be a prime element of K. If P is of the form $P = \pi Q$ for some $Q \in \mathcal{O}_K[x]$, the statement follows from the statement for Q. Hence we can assume P is not of the form $P = \pi G$. Write $P = P_1 P_2 \cdots P_l$, $P_i \in \mathcal{O}_K$, P_i irreducible.

If $n \le 3v_{\mathfrak{p}}(\operatorname{Disc} P)$, there are trivially at most $\#(\mathcal{O}_K/\mathfrak{p}^n) = |\mathfrak{p}^n|_{\mathfrak{p}}^{-1} \le |\operatorname{Disc} P|_{\mathfrak{p}}^{-3}$ roots. Assume $n > 3v_{\mathfrak{p}}(\operatorname{Disc} P)$. Let x be a root of $P(x) \equiv 0 \bmod \mathfrak{p}^n$. Let P_i be a factor for which $v_{\mathfrak{p}}(P_i(x))$ is maximal. By

$$\begin{aligned} v_{\mathfrak{p}}(P'(x)) &= v_{\mathfrak{p}}\Big(\sum_j P_j'(x) P_1(x) \cdots \widehat{P_j(x)} \cdots P_n(x)\Big) \\ &\ge \min_j (v_{\mathfrak{p}}(P(x)) - v_{\mathfrak{p}}(P_j(x))) \end{aligned}$$

and

$$\min(v_{\mathfrak{p}}(P'(x)), v_{\mathfrak{p}}(P(x))) \le v_{\mathfrak{p}}(\operatorname{Disc} P), \qquad v_{\mathfrak{p}}(P(x)) > v_{\mathfrak{p}}(\operatorname{Disc} P),$$

we have

$$\min_j (v_{\mathfrak{p}}(P(x)) - v_{\mathfrak{p}}(P_j(x))) \le v_{\mathfrak{p}}(\operatorname{Disc} P)$$

and hence

$$v_{\mathfrak{p}}(P_i(x)) \ge v_{\mathfrak{p}}(P(x)) - v_{\mathfrak{p}}(\operatorname{Disc} P) \ge n - v_{\mathfrak{p}}(\operatorname{Disc} P) \ge 2v_{\mathfrak{p}}(\operatorname{Disc} P) + 1.$$

On the other hand $\gcd(P_i(x), P_i'(x)) \mid \operatorname{Disc} P$, and thus

$$v_{\mathfrak{p}}(P_i'(x)) \le v_{\mathfrak{p}}(\operatorname{Disc} P).$$

By Hensel's lemma we can conclude that P_i is linear. Since $v_{\mathfrak{p}}(P_i(x)) \ge n - v_{\mathfrak{p}}(\operatorname{Disc} P)$, x is a root of

$$P_i(x) \equiv 0 \bmod \mathfrak{p}^{n - v_{\mathfrak{p}}(\operatorname{Disc} P)}.$$

Since P_i is linear and not divisible by $\mathfrak{p}$, it has at most one root in the ring $\mathcal{O}_K/\mathfrak{p}^{n - v_{\mathfrak{p}}(\operatorname{Disc} P)}$. There are at most $v_{\mathfrak{p}}(\operatorname{Disc} P)$ elements of $\mathcal{O}_K/\mathfrak{p}^n$ reducing to this root. Summing over all i we find that there are at most $l v_{\mathfrak{p}}(\operatorname{Disc} P)$ roots of $P(x) \equiv 0 \bmod \mathfrak{p}^n$ in $\mathbb{Z}/\mathfrak{p}^n$. Since $l \le \deg P$, the statement follows. ∎

For every non-zero $\mathfrak{m} \in I_K$, we define $h(\mathfrak{m})$ to be the positive integer generating $\mathfrak{m} \cap \mathbb{Z}$.

LEMMA A.2. *Let K be a number field. Let $\mathfrak{m}$ be a non-zero ideal of $\mathcal{O}_K$. Let $P \in \mathcal{O}_K[x]$ be a square-free polynomial. Then* $\{x \in \mathbb{Z} : P(x) \equiv 0 \bmod \mathfrak{m}\}$

is the union of at most $|\mathrm{Disc}\, P|^3 \tau_{\deg P}(\mathrm{rad}(h(\mathfrak{m})))$ *arithmetic progressions of modulus* $h(\mathfrak{m})$.

Proof. By Lemma A.1, for every $\mathfrak{p} \mid \mathfrak{m}$, the equation

$$P(x) \equiv 0 \bmod \mathfrak{p}^n$$

has at most $|\mathrm{Disc}\, P|_{\mathfrak{p}}^{-3} \deg P$ roots in $\mathcal{O}_K/\mathfrak{p}^n$. For any ideal $\mathfrak{a}$, the intersection of $\mathbb{Z}$ with a set of the form $\{x \in \mathcal{O}_K : x \equiv x_0 \bmod \mathfrak{a}\}$ is either the empty set or an arithmetic progression of modulus $h(\mathfrak{a})$. This is in particular true for $\mathfrak{a} = \mathfrak{p}^n$; the set $\{x \in \mathbb{Z} : x \equiv x_0 \bmod \mathfrak{p}^n\}$ is the union of at most $|\mathrm{Disc}\, P|_{\mathfrak{p}}^{-3} \deg P$ arithmetic progressions of modulus $h(\mathfrak{p}^n)$.

Now consider a rational prime p at least one of whose prime ideal divisors divides m. Write $m = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\cdots\mathfrak{p}_k^{n_k}\mathfrak{m}_0$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \mid p$, $\gcd(\mathfrak{m}_0, p) = 1$, $n_1/e_1 \geq \cdots \geq n_k/e_k$ and $e_1, \ldots, e_k$ are the ramification degrees of $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$. The set $\{x \in \mathbb{Z} : x \equiv x_0 \bmod \mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_k^{n_k}\}$ is the intersection of the sets $\{x \in \mathbb{Z} : x \equiv x_0 \bmod \mathfrak{p}_j^{n_j}\}$, $1 \leq j \leq k$. At the same time, it is a disjoint union of arithmetic progressions of modulus

$$h(\mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_k^{n_k}) = h(\mathfrak{p}_1^{n_1}).$$

As $\{x \in \mathbb{Z} : x \equiv x_0 \bmod \mathfrak{p}_1^{n_1}\}$ is the disjoint union of at most $|\mathrm{Disc}\, P|_{\mathfrak{p}}^{-3} \deg P$ arithmetic progressions of modulus $h(\mathfrak{p}_1^{n_1})$, it follows that

$$\{x \in \mathbb{Z} : x \equiv x_0 \bmod \mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_k^{n_k}\}$$

is the disjoint union of at most $|\mathrm{Disc}\, P|_{\mathfrak{p}}^{-3} \deg P$ arithmetic progressions of modulus $h(\mathfrak{p}_1^{n_1}) = h(\mathfrak{p}_1^{n_1}\ldots\mathfrak{p}_k^{n_k})$. The statement follows. ∎

LEMMA A.3. *Let* K *be a number field. Let* $\mathfrak{m}$ *be a non-zero ideal of* $\mathcal{O}_K$. *Let* $P \in \mathcal{O}_K[x, y]$ *be a non-constant and square-free homogeneous polynomial. Then the set*

$$S = \{(x, y) \in \mathbb{Z}^2 : \gcd(x, y) = 1,\ \mathfrak{m} \mid P(x, y)\}$$

is the union of at most $|\mathrm{Disc}\, P|^3 \tau_{2\deg P}(\mathrm{rad}(h(\mathfrak{m})))$ *disjoint sets of the form* $L \cap \{(x, y) \in \mathbb{Z}^2 : \gcd(x, y) = 1\}$, L *a lattice of index* $[\mathbb{Z}^2 : L] = h(\mathfrak{m})$.

Proof. Let $\mathfrak{p} \mid \mathfrak{m}$. Let $n = v_{\mathfrak{p}}(\mathfrak{m})$. Let $r_1, \ldots, r_k \in \mathcal{O}_K/\mathfrak{p}^n$ be the roots of $P(r, 1) \cong 0 \bmod \mathfrak{p}^n$. Let $r_1', \ldots, r_{k'}' \in \mathcal{O}_K/\mathfrak{p}^n$ be such roots of $P(1, r) \cong 0 \bmod \mathfrak{p}^n$ as satisfy $\mathfrak{p} \mid r$. Then the set of solutions to $P(x, y) \cong 0 \bmod \mathfrak{p}^n$ in $\{(x, y) \in \mathbb{Z}^2 : \mathfrak{p} \nmid \gcd(x, y)\}$ is the union of the disjoint sets

$$\{(x, y) \in \mathbb{Z}^2 : \mathfrak{p} \nmid \gcd(x, y),\ x \equiv r_i y \bmod \mathfrak{p}^n\},$$
$$\{(x, y) \in \mathbb{Z}^2 : \mathfrak{p} \nmid \gcd(x, y),\ y \equiv r_i x \bmod \mathfrak{p}^n\}.$$

The rest of the argument is as in Lemma A.2. ∎

LEMMA A.4. *Let* $S \subset \mathbb{R}^2$ *be a sector. Let* L *be a lattice not contained in* $\{(x, y) \in \mathbb{Z}^2 : \gcd(x, y) \neq 1\}$. *Then*

$$\#(\{-N \leq x, y \leq N : \gcd(x, y) = 1\} \cap S \cap L)$$

equals

$$\frac{\operatorname{Area}(S\cap[-N,N]^2)}{[\mathbb{Z}^2:L]}\prod_p\left(1-\frac{1}{p^2}\right)+O(N\log N).$$

The implied constant is absolute.

Proof. We can write $\#(\{1\le x,y\le N:\gcd(x,y)=1\}\cap S\cap L)$ as

$$\sum_{m=1}^{N}\mu(m)\#(\{1\le x,y\le N: m\,|\,x,\, m\,|\,y\}\cap S\cap L).$$

Since L is not of the form lL', $l>1$, $L'\subset\mathbb{Z}^2$ a lattice, we see that $m^{-1}(L\cap m\mathbb{Z}^2)$ is a lattice of index $[\mathbb{Z}^2:m^{-1}(L\cap m\mathbb{Z}^2)]=[\mathbb{Z}^2:L]$. Thus

$$\#(\{1\le x,y\le N: m\,|\,x,\, m\,|\,y\}\cap S\cap L)=AN^2/m^2[\mathbb{Z}^2:L]+O(N/m),$$

where $A=\operatorname{Area}(S\cap[-1,1]^2)$. Hence

$$\begin{aligned}\#(\{1\le x,y\le N&:\gcd(x,y)=1\}\cap S\cap L)\\ &=A\sum_{m=1}^{N}\mu(m)N^2/m^2[\mathbb{Z}^2:L]+O(N\log N)\\ &=\frac{\operatorname{Area}(S\cap[-N,N]^2)}{[\mathbb{Z}^2:L]}\prod_p\left(1-\frac{1}{p^2}\right)+O(N\log N).\ \blacksquare\end{aligned}$$

The following lemma is better than trivial estimates when L is a lattice of index greater than N.

Lemma A.5. *Let L be a lattice. Then*

$$\#(\{-N\le x,y\le N:\gcd(x,y)=1\}\cap L)\ll\frac{N^2}{[\mathbb{Z}^2:L]}+1.$$

Proof. Let $M_0=\min_{(x,y)\in L}\max(|x|,|y|)$. By [Gre, Lemma 1],

$$\#([-N,N]^2\cap L)\le\frac{4N^2}{[\mathbb{Z}^2:L]}+O\left(\frac{N}{M_0}\right).$$

If $M_0\ge[\mathbb{Z}^2:L]/(2N)$ we are done. Assume $M_0<[\mathbb{Z}^2:L]/(2N)$. Suppose

$$\#(\{-N\le x,y\le N:\gcd(x,y)=1\}\cap L)>2.$$

Let (x_0,y_0) be a point such that $\max(|x_0|,|y_0|)=M_0$. Let (x_1,y_1) be a point in $\{-N\le x,y\le N:\gcd(x,y)=1\}\cap L$ other than (x_0,y_0) and $(-x_0,-y_0)$. Since $\gcd(x_0,y_0)=\gcd(x_1,y_1)=1$, it cannot happen that 0, (x_0,y_0) and (x_1,y_1) lie on the same line. Therefore we have a non-degenerate parallelogram $(0,(x_0,y_0),(x_1,y_1),(x_0+x_1,y_0+y_1))$ whose area has to be at least $[\mathbb{Z}^2:L]$. On the other hand, its area can be at most $\sqrt{x_0^2+y_0^2}\sqrt{x_1^2+y_1^2}\le\sqrt{2}M_0\sqrt{2}N=2M_0N$. Since we have assumed $M_0<[\mathbb{Z}^2:L]/(2N)$ we arrive at a contradiction. $\blacksquare$

Appendix B. Divisor sums. Throughout the present paper, we use repeatedly, and sometimes without mention, the most common bounds on divisor functions: $\tau(n) \ll n^\varepsilon$, $\sum_{n=1}^N \tau_k(n) \ll N(\log N)^{k-1}$, $\sum_{n=1}^N \omega(n) \ll N \log\log N$, and so on. We also need the following auxiliary results, which are elementary but not quite standard.

Lemma B.1. *For every $\varepsilon > 0$,*

$$\sum_{n \text{ square-free}} \prod_{p|n} \frac{\log X}{p \log p} \ll X^\varepsilon,$$

where the implied constant depends only on ε.

Proof. For every positive k,

$$\begin{aligned}\sum_{p>k} \frac{1}{p\log p} &\leq \frac{1}{\log k}\left(\sum_{k\leq p<k^2} \frac{1}{p} + \frac{1}{2}\sum_{k^2\leq p<k^4} \frac{1}{p} + \frac{1}{4}\sum_{k^4\leq p<k^8} \frac{1}{p} + \cdots\right)\\ &= \frac{\log\log k^2 - \log\log k + O(1/(\log k))}{\log k}\\ &\quad + \frac{\log\log k^4 - \log\log k^2 + O(1/(\log k))}{2\log k} + \cdots\\ &= \frac{2(\log 2 + O(1/(\log k)))}{\log k}.\end{aligned}$$

Hence

$$\prod_{p>k}\left(1 + \frac{1}{p\log p}\right) \ll e^{2\log 2/\log k + O(1/(\log k)^2)}.$$

Now

$$\begin{aligned}\sum_{n \text{ square-free}} \prod_{p|n} \frac{\log X}{p\log p} &= \prod_{p\leq k}\left(1 + \frac{\log X}{p\log p}\right)\prod_{p>k}\left(1 + \frac{\log X}{p\log p}\right)\\ &\ll \prod_{p\leq k} \log X \prod_{p>k}\left(1 + \frac{1}{p\log p}\right)^{\log X}\end{aligned}$$

for $X > 2$. Therefore

$$\begin{aligned}&\sum_{n \text{ square-free}} \prod_{p|n} \frac{\log X}{p\log p} \ll e^{2\log 2\log X/\log k + O(\log X/(\log k)^2)} \prod_{p\leq k} \log X\\ &\ll \exp\left(\frac{2\log 2\log X}{\log k} + O\left(\frac{\log X}{(\log k)^2}\right)\right) \exp\left(\frac{k\log\log X}{\log k} + O\left(\frac{k\log\log X}{(\log k)^2}\right)\right).\end{aligned}$$

Set $k = \log X/\log\log X$. We obtain

$$\sum_{n\,\text{square-free}} \prod_{p|n} \frac{\log X}{p\log p} \ll e^{(2\log 2+\varepsilon')\log X/\log\log X}$$

for every $\varepsilon' > 0$, where the implied constant depends only on ε'. ∎

LEMMA B.2. *Let $c > 0$ be given. For every $\varepsilon > 0$,*

$$\frac{1}{N} \sum_{\substack{1\le n\le N\\ n\ \text{square-free}}} \tau(n) \prod_{p|n} \frac{c_0 \log N}{\log p} \ll N^{\varepsilon},$$

where the implied constant depends only on c_0 and ε.

Proof. Clearly

$$\frac{1}{N} \sum_{\substack{1\le n\le N\\ n\,\text{square-free}}} \tau(n) \prod_{p|n} \frac{c\log N}{\log p} \le \frac{1}{N} \sum_{\substack{1\le n\le N\\ n\,\text{square-free}}} \prod_{p|d} \frac{2c\log N}{\log p} \ll \sum_{n=1}^{\infty} \prod_{p|n} \frac{\log N^{2c}}{p\log p}.$$

Proceed as in Lemma B.1. ∎

References

[BK] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. 44 (1977), 715–743.

[Ca] J. W. S. Cassels, *The Mordell–Weil group of curves of genus* 2, in: Arithmetic and Geometry, Vol. I, Progr. Math. 35, Birkhäuser, Boston, 1983, 27–60.

[CF] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, London Math. Soc. Lecture Note Ser. 230, Cambridge Univ. Press, Cambridge, 1996.

[CHM] J. H. Conway, A. Hulpke and J. McKay, *On transitive permutation groups*, LMS J. Comput. Math. 1 (1998), 1–8.

[CS] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren Math. Wiss. 290, Springer, New York, 1988.

[Es] T. Estermann, *Einige Sätze über quadratfreie Zahlen*, Math. Ann. 105 (1931), 653–662.

[FPS] E. V. Flynn, B. Poonen and E. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-*2 *curve*, Duke Math. J. 90 (1997), 435–463.

[GAP4] The GAP Group, *GAP—Groups, Algorithms, and Programming, Version 4.3*, http://www.gap-system.org, 2002.

[Gre] G. Greaves, *Power-free values of binary forms*, Quart. J. Math. Oxford Ser. (2) 43 (1992), 45–65.

[GS] R. Gross and J. Silverman, *S-integer points on elliptic curves*, Pacific J. Math. 167 (1995), 263–288.

[He] H. A. Helfgott, *The distribution of the root number in families of elliptic curves*, preprint.

[He2] —, *Root numbers and the parity problem*, Ph.D. thesis, Princeton Univ., http://www.arxiv.org/abs/math.NT/0305435.

[Hoo] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Univ. Press, Cambridge, 1976.

[KL] G. A. Kabatjanskiĭ [G. A. Kabatyanskiĭ] and V. I. Levenšteĭn [V. I. Levenshteĭn], *Bounds for packings on the sphere and in space*, Problemy Peredachi Informatsii 14 (1978), no. 1, 3–25 (in Russian); English transl.: Problems of Information Transmission 14 (1978), no. 1, 1–17.

[La] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, New York, 1983.

[Maz] B. Mazur, *Rational points on modular curves*, in: Modular Functions of One Variable, V, Lecture Notes in Math. 601, Springer, Berlin, 1977.

[Mu] D. Mumford, *A remark on Mordell's conjecture*, Amer. J. Math. 87 (1965), 1007–1016.

[PT] A. Parson and J. Tull, *Asymptotic behavior of multiplicative functions*, J. Number Theory 10 (1978), 395–420.

[Ra] K. Ramsay, personal communication.

Département de mathématiques et de statistique
Université de Montréal
Montréal, QC H3C 3J7, Canada
E-mail: helfgott@dms.umontreal.ca

Received on 29.9.2003
and in revised form on 18.2.2004 (4637)