ON THE SQUARE-FREE SIEVE

H. A. HELFGOTT

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

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

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, $δ(P)$, 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:

| $\text{deg}_{\text{irr}}(P)$ | $δ(P(x))$ | $δ(P(x, y))$ |
|-----------------------------|-------------|--------------|
| 1                           | $\sqrt{N}$  | 1            |
| 2                           | $N^{2/3}$   | $N$          |
| 3                           | $N/(\log N)^{1/2}$ | $N^2/\log N$ |
| 4                           | $N^2/\log N$ | $N^2/\log N$ |
| 5                           | $N^2/\log N$ | $N^2/\log N$ |
| 6                           | $N^2/(\log N)^{1/2}$ | $N^2/(\log N)^{1/2}$ |

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

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

1991 Mathematics Subject Classification. 11N32 (primary); 11N36, 11G05.
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 the prime divisors of $n$, and $\text{rad}(n)$ for the product of the prime divisors of $n$. Given a prime $p$, we write $\nu_p(n)$ for the non-negative integer $j$ such that $p^j | n$ and $p^{j+1} \nmid n$. For any $k \geq 2$, we write $\tau_k(n)$ for the number of $k$-tuples $(n_1, n_2, \ldots, n_k) \in (\mathbb{Z}^+)^k$ such that $n_1 \cdot n_2 \cdots n_k = |n|$. Thus $\tau_2(n) = \tau(n)$. We adopt the convention that $\tau_1(n) = 1$. We let

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

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

We denote by $\mathcal{O}_K$ the ring of integers of a global or local field $K$. We let $I_K$ be the semigroup of non-zero ideals of $\mathcal{O}_K$. Given a non-zero ideal $a \in I_K$, we write $\tau_K(a)$ for the number of ideals dividing $a$, $\omega_K(a)$ for the number of prime ideals dividing $a$, and $\text{rad}_K(a)$ for the product of the prime ideals dividing $a$. Given a positive integer $k$, we write $\tau_{K,k}(a)$ for the number of $k$-tuples $(a_1, a_2, \ldots, a_k)$ of ideals of $\mathcal{O}_K$ such that $a = a_1 a_2 \cdots a_k$. Thus $\tau_2(a) = \tau(a)$. We define $\rho(a)$ to be the positive integer generating $a \cap \mathbb{Z}$.
When we say that a polynomial $f \in \mathcal{O}_K[x]$ 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 $g^2 | f$.

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 $\text{rank}(E)$ 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 will always mean an additive subgroup of $\mathbb{Z}^2$ of finite index. For $S \subset [-N, N]$ a convex set and $L$ a lattice,

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

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:

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

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 $p^2 \not | P(x)$, where $P(x)$ is a fixed polynomial with integer coefficients. Thus we know that we are being asked to evaluation 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 \( p^2|F(x) \) (see section 5). In other instances, the full generality of our treatment becomes necessary: see [He] for the example

\[
(3.2) \quad u(n) = \prod_p u_p(n) = \prod_p \frac{W_p(\mathcal{E}(n))}{W_{0,p}(\mathcal{E}(n))},
\]

where \( \mathcal{E} \) 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 \( \epsilon > 0 \), there is a partition \( \mathbb{Z}_p = U_0 \cup U_1 \cup \ldots \cup U_k \) and a tuple of complex numbers \((y_1, \ldots, y_k)\) such that

1. \( |f(x) - y_j| < \epsilon \) for \( x \in U_j \), \( 1 \leq j \leq k \),
2. \( \text{meas}(U_0) < \epsilon \),
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 \( |u_p(x)| \leq 1 \) for every \( x \in \mathbb{Z}_p \). Assume that \( u_p(x) = 1 \) unless \( p^2|P(x) \), where \( P \in \mathbb{Z}[x] \) is a polynomial satisfying

\[
\#\{1 \leq x \leq N : \exists p > N^{1/2}, p^2|P(x, y)\} = o(N).
\]

Let \( u(n) = \prod_p u_p(n) \). Then (3.2) 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 [Hod], Ch. IV, and [Gre]. Let \( \epsilon_0 \) 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

\[
\left| \prod_p \int_{\mathbb{Z}_p} u_p(x)dx - \prod_{p \leq \epsilon_0^{-1}} \int_{\mathbb{Z}_p} u_p(x)dx \right| = O(\epsilon_0).
\]

Let

\[
u'(x) = \prod_{p \leq \epsilon_0^{-1}} u_p(x).
\]
Since \( u'(x) = u(x) \) unless \( p^2|P(x) \) for some \( p > \epsilon_0^{-1} \),
\[
\left| \sum_{n=1}^{N} u(n) - \sum_{n=1}^{N} u'(n) \right| \leq 2 \cdot \# \{ 1 \leq x \leq N : \exists p > \epsilon_0^{-1} \text{ s.t. } p^2|P(x) \} \\
\leq 2 \sum_{\epsilon_0^{-1} < p \leq N^{1/2}} \sum_{1 \leq x \leq N} 1 \\
+ 2 \cdot \# \{ 1 \leq x \leq N : \exists p > N^{1/2}, p^2|P(x) \}.
\]

By Appendix A, Lemma A.2,
\[
\sum_{\epsilon_0^{-1} < p \leq N^{1/2}} \sum_{1 \leq x \leq N} 1 = O \left( \sum_{\epsilon_0^{-1} < p \leq N^{1/2}} N/p^2 \right) = O(\epsilon_0 N),
\]
where the implied constant depends only on \( P \). By the assumption in the statement,
\[
\# \{ 1 \leq x \leq N : \exists p > N^{1/2}, p^2|P(x) \} \leq \epsilon_0 N
\]
for \( N \) greater than some constant \( C_{\epsilon_0} \). It now remains to compare
\[
\frac{1}{N} \sum_{n=1}^{N} u'(n) \quad \text{and} \quad \prod_{p < \epsilon_0} \int_{Z_p} u_p(x) \, dx.
\]

For every \( p \), we are given a tuple \( (y_1, \ldots, y_{k_p}) \) and a partition \( Z_p = U_{p,0} \cup U_{p,1} \cup \cdots \cup U_{p,k_p} \) satisfying the conditions in Definition 1 with \( \epsilon = \epsilon_0^2 \). We can assume that \( U_{p,1}, U_{p,2}, \ldots, U_{p,k_p} \) are connected and \( |y_1|, \ldots, |y_{k_p}| \leq 1 \). We have
\[
\sum_{n=1}^{N} u'(n) = \sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} \sum_{1 \leq n \leq N} \left( \prod_{p < \epsilon_0^{-1}} y_{p,j_p} + O \left( (1 + \epsilon_0^2 \epsilon_0^{-1}) - 1 \right) \right) \\
= \sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} \sum_{1 \leq n \leq N} \prod_{p < \epsilon_0^{-1}} y_{p,j_p} + O(\epsilon_0 N) \\
= \sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} \sum_{1 \leq n \leq N} \prod_{p < \epsilon_0^{-1}} y_{p,j_p} \cdot \# \{ 1 \leq n \leq N : n \in \bigcap_{p} U_{p,j_p} \cap Z \} \\
+ O(\epsilon_0 N),
\]
whereas
\[
\prod_{p < \epsilon_0} \int_{\mathbb{Z}_p} u_p(x) \, dx = \sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} \prod_{p < \epsilon_0} \int_{U_{p,j_p}} u_p(x) \, dx
\]
\[
= \sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} \prod_{p < \epsilon_0} \text{meas}(U_{p,j_p})(y_{p,j_p} + O(\epsilon)).
\]

The absolute value of
\[
\sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} \prod_{p < \epsilon_0^{-1}} \text{meas}(U_{p,j_p})(y_{p,j_p} + O(\epsilon)) - \sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} \prod_{p < \epsilon_0^{-1}} \text{meas}(U_{p,j_p})y_{p,j_p}
\]
is at most a constant times
\[
\sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} \left( \prod_{p < \epsilon_0^{-1}} \text{meas}(U_{p,j_p})(1 + \epsilon) - \prod_{p < \epsilon_0^{-1}} \text{meas}(U_{p,j_p}) \right)
\]
\[
\ll \prod_{p < \epsilon_0^{-1}} (1 + \epsilon) - 1 \ll \epsilon_0.
\]

It is left to bound the difference between
\[
\frac{1}{N} \sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} y_{p,j_p} \cdot \# \{1 \leq n \leq N : n \in \bigcap_{p} U_{p,j_p} \cap \mathbb{Z}\}
\]
and
\[
\sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} \prod_{p < \epsilon_0^{-1}} \text{meas}(U_{p,j_p})y_{p,j_p}.
\]

It is enough to estimate
(3.3)
\[
\sum_{\vec{j} \in \prod_{p < \epsilon_0^{-1}} [0, k_p]} \left( \prod_{p < \epsilon_0^{-1}} \text{meas}(U_{p,j_p}) - \frac{1}{N} \# \{1 \leq n \leq N : n \in \bigcap_{p} U_{p,j_p} \cap \mathbb{Z}\} \right).
\]

When all \(j_p\) are positive, \(\bigcap_{p} U_{p,j_p} \cap \mathbb{Z}\) is an arithmetic progression. Hence
\[
N \prod_{j} \text{meas}(U_{p,j_p}) - \# \{1 \leq n \leq N : n \in \bigcap_{p} U_{p,j_p} \cap \mathbb{Z}\} \leq 1.
\]

When some \(j_p\) are zero, we can use inclusion-exclusion to obtain
\[
\left| \# \{1 \leq n \leq N : n \in \bigcap_{p} U_{p,j_p} \cap \mathbb{Z}\} - N \prod_{j} \text{meas}(U_{p,j_p}) \right| \leq \prod_{j_p=0} k_p.
\]

Hence the absolute value of (3.3) is at most
\[
\frac{1}{N} \prod_{p < \epsilon_0^{-1}} (2k_p).
\]
If $N > \epsilon_0^{-1} \prod_{p<\epsilon_0} (2k_p)$, then clearly $\frac{1}{N} \prod_{p<\epsilon_0} (2k_p) = O(\epsilon_0)$.

We can conclude that, for $N \geq \max(C_{\epsilon_0}, \epsilon_0^{-1} \prod_{p<\epsilon_0} (2k_p))$,

$$\lim_{N \to \infty} \left| \sum_{n=1}^{N} u(n) - \prod_{p} \int_{Z_p} u_p(x) \, dx \right| = O(\epsilon_0),$$

where the implied constant depends only on $P$. \hfill \Box

The question now is to make Prop. 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 $P(\mathcal{P})$ for the set of all subsets of a given set $\mathcal{P}$.

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

The purpose of a sieve is to estimate

(3.4) \[ \sum_{a \in \mathcal{A}} f(a, r(a)) \]

given data on

(3.5) \[ \sum_{a \in \mathcal{A}} f(a, d_2) \]

for $d_1, d_2 \in P(\mathcal{P})$. 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 $\mathcal{P}$. We will take as given a function $h : P(\mathcal{P}) \to \mathbb{Z}^+$ such that

(h1) \[ h(d_1 \cup d_2) \leq h(d_1) h(d_2) \] for all $d_1, d_2 \in P(\mathcal{P})$ disjoint.

and

(h2) \[ \{ d \in P(\mathcal{P}) : h(d) \leq n \} \text{ is finite for every } n \in \mathbb{Z}. \]

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

(A1) \[ \sum_{a \in \mathcal{A}} \frac{1}{r(a) \supset d} \leq C_0 \frac{XC^\#d}{h(d)} + C_0 C^\#d_2 \text{ for } d \subset \mathcal{P}, \]

(A2) \[ \sum_{a \in \mathcal{A}} f(a, d_2) = \frac{g(d_1, d_2)}{h(d_1)} + r_{d_1, d_2} \text{ for } d_2 \subset d_1 \subset \mathcal{P}, \text{ and } h(d) \leq M_0. \]
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.

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

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

$$\left| \sum_{a \in \mathcal{A}} f(a, r(a)) - \sum_{d \in \mathcal{P}} \sum_{d' \subseteq d, h(d) \leq M} \mu(d - d') A_{d,d'} \right|$$

is at most

$$\left( \sum_{d \in \mathcal{P}, M < h(d) \leq M^2} (3^{\#d} + 3) S_d + \sum_{p \in \mathcal{P}, h(\{p\}) > M^2} S_{\{p\}} \right) \cdot \max_{a,d} f(a, d).$$

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

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

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

$$\sum_{a \in \mathcal{A}} f(a, r(a)) = \sum_{a \in \mathcal{A}} (f(a, r(a)) - f(a, \pi(r(a)))) + \sum_{a \in \mathcal{A}} \delta_a$$

$$+ \sum_{d \subseteq \mathcal{P}} \sum_{d' \subseteq d, h(d) \leq M} \mu(d - d') A_{d,d'},$$

where we write

$$\delta_a = \sum_{d \subseteq r(a)} \sum_{d' \subseteq d, x \in d \Rightarrow h(\{x\}) \leq M} \mu(d - d') f(a, d') - \sum_{d \subseteq r(a)} \sum_{d' \subseteq d, h(d) \leq M} \mu(d - d') f(a, d').$$

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

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

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

$$\sum_{d \subset r(a)} \sum_{d' \subset d, h(d) \leq M} \mu(d - d') f(a, d') \leq \max_{a,d} |f(a, d)| \cdot \sum_{d \subset r(a), h(d) \leq M} 2^{|d|}.$$ 

By the foregoing discussion,

$$\sum_{d \subset r(a), h(d) \leq M} 2^{|d|} \leq \sum_{s \subset r(a), M < h(s) \leq M^2} \sum_{d \subset s} 2^{|d|} = \sum_{s \subset r(a), M < h(s) \leq M^2} 3^{|s|}.$$ 

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

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

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

$$\sum_{s \subset r(a), M < h(s) \leq M^2} 1 \geq 1,$$

we can conclude that

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

Clearly

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

The statement follows. \hfill \square

**Corollary 3.3.** Let $(\mathcal{P}, \mathcal{A}, r, f)$ be a soil with $\max_{a,d} f(a, d) \leq C_5$. 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 $M \leq M_0$,

$$\left| \sum_{a \in \mathcal{A}} f(a, r(a)) - X \cdot \sum_{d \subset \mathcal{P}} \sum_{d' \subset d} \mu(d - d') \frac{g(d, d')}{h(d)} \right|.$$
is at most\[ X \sum_{d \in \mathcal{P}} \frac{1}{h(d)} \left( C_4 2^{\#d} + C_3 C_0 C_1^{\#d} (3^{\#d} + 3) \right) + C_3 \cdot \sum_{d \in \mathcal{P}} C_0 C_2^{\#d} (3^{\#d} + 3) \]
\[ + \sum_{d \in \mathcal{P}} \sum_{d' \subset d \atop h(d) \leq M} |r_d, d'| + C_3 \sum_{p \in \mathcal{P}} S_{\{p\}}. \]

(3.7)

**Proof.** Apply Proposition 3.2. By (A1),
\[ \sum_{d \in \mathcal{P}} (3^{\#d} + 3) S_d \leq X \cdot \sum_{d \in \mathcal{P}} C_0 C_1^{\#d} (3^{\#d} + 3) \]
\[ + \sum_{d \in \mathcal{P}} C_0 C_2^{\#d} (3^{\#d} + 3). \]

By (A2),
\[ \sum_{d \in \mathcal{P}} \sum_{d' \subset d \atop h(d) \leq M} \mu(d - d') A_{d, d'} = X \cdot \sum_{d \in \mathcal{P}} \sum_{d' \subset d \atop h(d) \leq M} \mu(d - d') \frac{g(d, d')}{h(d)} \]
\[ + \sum_{d \in \mathcal{P}} \sum_{d' \subset d \atop h(d) \leq M} \mu(d - d') r_{d, d'}. \]

Finally,
\[ \left| \sum_{d \in \mathcal{P}} \sum_{d' \subset d \atop h(d) > M} \mu(d - d') \frac{g(d, d')}{h(d)} \right| \leq \sum_{d \in \mathcal{P}} \frac{C_4 2^{\#d}}{h(d)}. \]

\[ \square \]

**Proposition 3.4.** Let $K$ be a number field. Let $Q \in \mathcal{O}_K[x]$ be a polynomial. Let $m$ be a positive integer. Then the number of positive integers $x \leq N$ for which $Q(x)$ is free of $m$th powers equals
\[ N \prod_p \left( 1 - \frac{\ell(p^m)}{p^m} \right) + O(N^{2/(m+1)} (\log N)^C) \]
\[ + O(\# \{ 1 \leq x \leq N : \exists p > N^{2/m+1} \text{ s.t. } p^m | Q(x) \}), \]

where
\[ \ell(p^m) = \# \{ x \in \mathbb{Z}/p^m : p^m | Q(x) \text{ for some } p \in I_K \text{ above } p \}. \]
The implied constant and $C$ depend only on $K$ and $Q$. 
Proof. We define a soil \((\mathcal{P}, \mathcal{A}, r, f)\) by
\[
\mathcal{P} = \{ p \in I_K : p \text{ prime} \}, \quad \mathcal{A} = \{1, 2, \ldots, N\},
\]
\[
r(a) = \{ p \in P : p^m | Q(a) \}, \quad f(a, d) = \begin{cases} 1 & \text{if } d = \emptyset, \\ 0 & \text{otherwise}. \end{cases}
\]

Let \(h(d)\) be the positive integer generating the ideal \((\prod_{p \in \mathcal{P}} p^m) \cap \mathbb{Z} \). Properties (h1) and (h2) are clear. Lemma [A.2] gives us properties (A1) and (A2) with
\[
X = N, \quad g(d_1, d_2) = 0 \text{ if } d_2 \text{ non-empty},
\]
\[
g(d, \emptyset) = \# \{ x \in \mathbb{Z} / h(d) : p^m | Q(x) \forall p \in d \},
\]
\[
|r_d, 0| = | \text{Disc} Q |^{3 \deg Q}_{d} |^{\# d}, \quad |r_{d_1, d_2}| = 0 \text{ if } d_2 \text{ non-empty},
\]
\[
C_0 \ll | \text{Disc} Q |^{3}, \quad C_1, C_2 \ll \deg Q, \quad M_0 = N.
\]

By Corollary 3.3, \(\sum_{a \in \mathcal{A}} f(a, r(a)) - N \sum_{d \subseteq \mathcal{P}} \sum_{d' \in d} \mu(d - d') \frac{g(d, d')}{h(d)}\) is at most
\[
N \cdot \sum_{d \subseteq \mathcal{P}} \sum_{h(d) > M} \frac{1}{h(d)} (2^{\# d} + C_0 C_1^{\# d} (3^{\# d} + 3)) + \sum_{d \subseteq \mathcal{P}} \sum_{M < h(d) \leq M^2} \frac{C_0 C_1^{\# d}}{M} (3^{\# d} + 3)
\]
\[
+ \sum_{d \subseteq \mathcal{P}} | \text{Disc} Q |^{3 \deg Q}_{d} \quad + \sum_{p \in \mathcal{P}} S_{p}.
\]

Given a positive integer \(n\), there are at most \(2^{(\deg K/Q)\omega(n)}\) elements \(d\) of \(\mathcal{P}\) such that \(h(d) = m\). Moreover, for every prime \(p\) not ramified in \(K/Q\), \(p|h(d)\) implies \(p^m|h(d)\). Hence
\[
N \cdot \sum_{d \subseteq \mathcal{P}} \sum_{h(d) > M} \frac{e^{\# d}}{h(d)} \ll N \cdot \sum_{n > M^{1/m}} \frac{2^{(\deg K/Q)\omega(n)}}{n^m} \ll N \frac{(\log M)^2 2^{\deg K/Q_{c-1}}}{M^{(m-1)/m}},
\]
\[
\sum_{d \subseteq \mathcal{P}} \frac{e^{\# d}}{M^{2/m}} \ll \sum_{d \subseteq \mathcal{P}} \frac{e^{\# d}}{M^{1/m}} \ll M^{2/m} (\log M)^{2^{c-1}}.
\]

We choose \(M = N^{m/m+1}\), since then \(\frac{N}{M^{(m-1)/m}} = M^{2/m}\). It remains to show that
\[
\sum_{d \subseteq \mathcal{P}} \sum_{d' \in d} \mu(d - d') \frac{g(d, d')}{h(d)} = \prod_p \left(1 - \frac{\ell(p^m)}{p^m}\right).
\]

By [5.2],
\[
\sum_{d \subseteq \mathcal{P}} \sum_{d' \in d} \mu(d - d') \frac{g(d, d')}{h(d)} = \sum_{d \subseteq \mathcal{P}} \mu(d) \frac{g(d, 0)}{h(d)} = \prod_p \sum_{d \subseteq \mathcal{P}} \mu(d) \frac{g(d, 0)}{h(d)} = \prod_{p \text{ prime}} \left(1 - \frac{\ell(p^m)}{p^m}\right)
\]
and so we are done. \(\square\)
While the following result could be stated in the same generality as Prop. 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 \( x, y \leq N \) for which \( Q(x, y) \) is free of \( m \)th powers equals

\[
N^2 \prod_p \left( 1 - \frac{\ell(p^2)}{p^4} \right) + O(N^{3/2} (\log N)^C)
\]

and

\[
+ O\left( \{1 \leq x, y \leq N : \exists p > N \text{ s.t. } p^2 | Q(x, y) \} \right),
\]

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 \((\mathcal{P}, \mathcal{A}, r, f)\) by

\[
\mathcal{P} = \{ p \in \mathbb{Z}^+ : p \text{ prime} \}, \quad \mathcal{A} = \{ 1 \leq x, y \leq N : \gcd(x, y) = 1 \},
\]

\[
r(a) = \{ p \in \mathcal{P} : p^2 | Q(a) \}, \quad f(a, d) = \begin{cases} 1 & \text{if } d \neq \emptyset, \\ 0 & \text{otherwise.} \end{cases}
\]

Let \( h(d) = \prod_{p \in d} p^2 \). Properties (h1), (h2), (A1) and (A2) hold by Lemmas A.3, A.4 and A.5 with

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

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

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

\[
C_0 \ll |\text{Disc } Q|^3, \quad C_1, C_2 = 2 \deg Q, \quad M_0 = N.
\]

By Corollary 3.3

\[
\sum_{a \in \mathcal{A}} f(a, r(a)) - X \sum_{d \in \mathcal{P}} \sum_{d' \subset d} \mu(d - d') g(d) \text{ is at most}
\]

\[
N^2 \prod_p \left( 1 - \frac{1}{p^2} \right) \sum_{n > M^{1/2}} \frac{1}{n^2} (2^{\omega(n)} + C_0 C_1 (3^{\omega(n)} + 3)) + \sum_{p \text{ prime} \atop p > M} S_p
\]

\[
+ \sum_{M^{1/2} < n \leq M} C_0 C_2 (3^{\omega(n)} + 3) + \sum_{n \leq M^{1/2}} |\text{Disc } Q|^3 (2 \deg Q)^{\omega(n)} N \log N,
\]

which is in turn at most

\[
N^2 \frac{(\log M)^C}{M^{1/2}} + M (\log M)^C + M^{1/2} N \log N + \sum_{p \text{ prime} \atop p > M} S_p
\]

for some \( C \) given by \( C_0, C_1, C_2 \). We set \( M = N \). Now

\[
\sum_{d \subset \mathcal{P}} \sum_{d' \subset d} \mu(d - d') \frac{g(d, d')}{h(d)} = \sum_{d \subset \mathcal{P}} \mu(d) \frac{g(d, \emptyset)}{h(d)} = \prod_p \left( 1 - \frac{\ell'(p^2)}{p^4} \right),
\]
where \( \ell'(p^2) = \# \{ x, y \in \mathbb{Z}/p^2 : p^2 | Q(x, y) \land (p \not| x \lor p \not| y) \} / (p^2 - 1) \). Clearly \( \ell'(p^2)(p^2 - 1) = \ell(p^2) - p^2 \). Hence

\[
\prod_p \left( 1 - \frac{\ell'(p^2)}{p^2} \right) = \prod_p \left( 1 - \frac{\ell(p^2) - p^2}{p^2(p^2 - 1)} \right) = \prod_p \frac{p^4 - \ell(p^2)}{p^2(p^2 - 1)} = \prod_p \left( 1 - \frac{\ell(p^2)}{p^4} \right) / \prod_p \left( 1 - \frac{1}{p^2} \right).
\]

The statement follows. \( \square \)

### 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 \( \mu_j, j \in J_0 \). Consider a countable set \( Z \) together with injections \( \iota_j : Z \to V_j \) for every \( j \in J_0 \), and a finite subset \( Z_n \subseteq Z \) for every \( n \in \mathbb{Z}^+ \). Let \( \mathcal{M} \) be a collection of measurable subsets of \( V_j \), each of them of finite measure. Let \( v : \mathbb{Z}^+ \to \mathbb{R}_0^+ \) be a function with \( \lim_{n \to \infty} v(n) = 0 \). Assume that

\[
\left| \frac{1}{\# Z_n} \sum_{x \in Z_n \cap \bigcap_{j \in J} \iota_j^{-1}(M_j)} \left( 1 - \prod_{j \in J} \mu_j(M_j) \right) \right| \leq v(n)
\]

for every finite subset \( J \subseteq J_0 \) and every tuple \( \{ M_j \}_{j \in J}, M_j \in \mathcal{M} \).

We may call \( Z \) the sample frame, and \( \mathcal{M}, j \in J_0 \), the sampling spaces. A tuple \( (J_0, \{ V_j \}, Z, \{ \iota_j \}, \{ Z_n \}, v, \{ \mathcal{M} \}) \) satisfying the conditions above, including (3.8), will be called a sampling datum. Given a measure \( \sigma_j \) 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 \( \max(|s_j(x)|) \leq 1 \), \( \max |\sigma_j/\mu_j| \leq 1 \), and

\[
\left| \frac{1}{\# Z_n} \sum_{x \in Z_n \cap \bigcap_{j \in J} \iota_j^{-1}(M_j)} s(x) - \prod_{j \in J} \sigma_j(M_j) \right| \leq v_0(n) \prod_{j \in J} \mu_j(M_j) + v_1(n)
\]

for every finite subset \( J \subseteq J_0 \) and every tuple \( \{ M_j \}_{j \in J}, M_j \in \mathcal{M} \), where \( v_0(n), v_1(n) : \mathbb{Z}^+ \to \mathbb{R}_0^+ \) are functions with \( \lim_{n \to \infty} v_0(n) = \lim_{n \to \infty} v_1(n) = 0 \) and we write \( s(x) \) for \( \prod_{j \in J} s_j(x) \).

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

\[
(M_1 \cup M_2 \cup \cdots \cup M_n) - (M'_1 \cup \cdots \cup M'_{n_2}),
\]

where \( M_1, \ldots, M_n \in \mathcal{M} \) and \( M'_1, \ldots, M'_{n_2} \in \mathcal{M} \) and \( n_1 + n_2 \leq c \). It should be clear that (3.8) and the inequality following it hold for \( M_j \in \mathcal{M}_{c,j} \) if the terms on the right are multiplied by \( c^{\#J} \).

Let \( j \) be an element of \( J_0 \). Let \( M_j \in \mathcal{M} \). 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 \( M_j = M_{j,0} \cup M_{j,1} \cup M_{j,2} \cup \cdots \) and a sequence \( \{ y_i \}_{i \geq 1} \) of complex numbers such that

1. \( M_{j,i} \in \mathcal{M}_{c,j} \) for \( i \geq 1 \),
(2) \( f(x) = y_i \) for \( x \in U_i, \ i \geq 1 \),

(3) \( \mu_j(M_{j,0}) = 0 \),

(4) \( \mu_j(M_{j,i}) \leq m(i) \) for every \( i \geq 1 \).

**Lemma 3.6.** Let \((J_0, \{V_j\}, Z, \{t_j\}, \{Z_n\}, \nu, \{M_j\})\) be a sampling datum, \((s_j, \sigma_j)\) a distribution pair. Let \( J \) be a finite subset of \( J_0 \). For every \( j \in J \), choose \( M_j \in M_j \) and let \( u_j : M_j \rightarrow C \) be a \((c, m_j)\)-approximable function with \( \max_x |u_j(x)| \leq 1 \). 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 \((\mathbb{Z}^+)^J\),

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

is at most

\[
\sum_{(t_j) \in (\mathbb{Z}^+)^J - S} \prod_{j \in J} m_j(t_j) + c_0 v_0(n) \prod_{j \in J} \mu_j(M_j) + \#S \cdot c_0 v_1(n) + (\#S + 1)c_0 v(n).
\]

**Proof.** Since \(|\sigma_j/\mu_j| \leq 1, |u_j| \leq 1 \) and \( u_j \) is \( m_j \)-approximable,

\[
\left| \prod_{j \in J} \int_{M_j} u_j(x) d\sigma_j - \sum_{(t_j) \in S} \prod_{j \in J} \int_{M_j, t_j} u_j(x) d\sigma_j \right| = \left| \sum_{(t_j) \in (\mathbb{Z}^+)^J - S} \prod_{j \in J} \int_{M_j, t_j} u_j(x) d\sigma_j \right| \leq \sum_{(t_j) \in (\mathbb{Z}^+)^J - S} \prod_{j \in J} m_j(t_j),
\]

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

\[
\left| \prod_{j \in J} \sigma_j(M_{j, t_j}) - \frac{1}{\#Z_n} \sum_{x \in Z_n \cap \bigcap_{j \in J} V_j} s(x) \right|
\]

is at most

\[
c_0 v_0(n) \prod_{j \in J} \mu_j(M_{j, s_j}) + c_0 \cdot v_1(n).
\]

Clearly

\[
\sum_{(t_j) \in S} c_0 v_0(n) \prod_{j \in J} \mu_j(M_{j, t_j}) = c_0 v_0(n) \sum_{(t_j) \in (\mathbb{Z}^+)^J} \prod_{j \in J} \mu_j(M_{j, t_j}) = c_0 v_0(n) \prod_{j \in J} \mu_j(M_j).
\]
By (3.8),

\[ \left| \sum_{(t_j) \notin S} \frac{1}{\#Z_n} \sum_{x \in Z_n \cap \cap_{j \in J} t_j^{-1}(M_{j,t_j})} s(x) \right| \leq \sum_{(t_j) \notin S} \frac{1}{\#Z_n} \sum_{x \in Z_n \cap \cap_{j \in J} t_j^{-1}(M_{j,t_j})} 1 \\
= \frac{\#(Z_n \cap \cap_{j \in J} t_j^{-1}(M_j))}{\#Z_n} \\
- \sum_{(t_j) \in S} \frac{1}{\#Z_n} \sum_{x \in Z_n \cap \cap_{j \in J} t_j^{-1}(M_{j,t_j})} 1 \\
= \prod_{j \in J} \mu_j(M_j) - \sum_{(t_j) \in S} \prod_{j \in J} \mu_j(M_{j,t_j}) \\
+ O(c_0 \cdot (\#S + 1)v(n)) \\
= \sum_{(t_j) \in (\mathbb{Z}^+) \setminus S} \prod_{j \in J} \mu_j(M_{j,t_j}) \\
+ O(c_0 \cdot (\#S + 1)v(n)). \]

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

It is time to produce some examples of sampling data.

**Example 1.** Let \( J_0 \) be the set of rational primes. Let \( V_p = \mathbb{Z}_p \), \( Z = \mathbb{Z} \), \( Z_n = \{1, 2, \ldots, n\} \), \( \iota_p : \mathbb{Z} \to \mathbb{Z}_p \) the natural injection, \( \mathcal{M}_p \) the set of additive subgroups of \( \mathbb{Z}_p \) of finite index, \( v(n) = 1/n \). Then

\[ (J_0, \{V_p\}, Z, \{\iota_p\}, \{Z_n\}, v, \{\mathcal{M}_p\}) \]

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 \( V_p = \mathbb{Z}_p^2 \), \( Z = \mathbb{Z}^2 \cap S \), \( Z_n = \{-n \leq x, y \leq n\} \cap S \), \( \iota_p : \mathbb{Z} \to \mathbb{Z}_p \) the natural injection, \( v(n) = O(1/n) \), \( \mathcal{M}_p \) the set of all additive subgroups of \( \mathbb{Z}_p^2 \) of finite index. Then \((J_0, \{V_p\}, Z, \{\iota_p\}, \{Z_n\}, v, \{\mathcal{M}_p\})\) 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 \( V_p = \mathbb{Z}_p^2 - p\mathbb{Z}_p^2 \), \( Z = \{x, y \in \mathbb{Z} : \gcd(x, y) = 1\} \cap S \), \( Z_n = \{-n \leq x, y \leq n : \gcd(x, y) = 1\} \cap S \), \( v(n) = O(\log n/n) \), \( \mathcal{M}_p \) 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 \([A.4]\) \((J_0, \{V_p\}, Z, \{\iota_p\}, \{Z_n\}, v, \{\mathcal{M}_p\})\) 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 $(c_0, c_1 p^{-c_2})$-approximable function, where $c_0$ is a positive integer and $c_1$, $c_2$ are positive real numbers. Assume that $|u_p(x)| \leq 1$ for every $x \in \mathbb{Z}_p$. Assume, furthermore, that $u_p(x) = 1$ unless $p^2 | P(x)$, where $P \in \mathbb{Z}[x]$ is a fixed square-free polynomial. Then

$$
\frac{1}{N} \sum_{n=1}^{N} \prod_{p} u_p(n) = \prod_{p} \int_{\mathbb{Z}_p} u_p(x) dx + O((\log N)N^{-1/3})
$$

$$
+ \frac{1}{N} O\{1 \leq x \leq N : \exists p > N^{2/3} \text{ s.t. } p^2 | P(x)\},
$$

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

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

$$
\mathcal{P} = \{ p \in \mathbb{Z}^+ : p \text{ prime} \}, \quad \mathcal{A} = \{1, 2, \ldots, N\},
$$

$$
r(a) = \{ p \in \mathcal{P} : p^2 | P(a) \}, \quad f(a, d) = \prod_{p \in d} u_p(a).
$$

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

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

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

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

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

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

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

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

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

$$
(3.10) \quad S = \chi_{p^{d_1}} \{ n \in \mathbb{Z} : 1 \leq n \leq \frac{c_2 \log N}{\log p} \}.
$$

Then

$$
\sum_{(s_p) \in (\mathbb{Z}^+)^{d_1 - S}} \prod_{p \in d_1} m_p(s_p) \leq \sum_{p \in d_1} \sum_{j > \frac{c_2 \log N}{\log p} \log p} m_p(j)
$$

$$
\leq \sum_{p \in d_1} \frac{c_1}{1 - p^{-c_2}} e^{- \frac{c_2 \log N}{\log p}} = \frac{c_1}{1 - 2^{-c_2}} \cdot \#^{d_1}/N,
$$
and so
\[ r_{d_1,d_2} \leq 2c_0^{\#d_1} \prod_{p \in d_1} \left( c_2 \log N \frac{\log p}{\log p} \right) + \frac{c_1}{1 - 2^{-c_2}} \cdot \#d_1 + c_0^{\#d_1}. \]

We can now apply Corollary 3.3. We obtain that the absolute value of the difference
\[
\sum_{a \in S} f(a, r(a)) - N \cdot \sum_{d} \sum_{d' \leq d} \mu(d-d') \frac{g(d,d')}{h(d)}
\]
\[= \sum_{n=1}^{N} \prod_{p} u_p(n) - N \cdot \sum_{d \text{ sq-free}} \sum_{d' \leq d} \mu(d/d') \prod_{p|d/d'} \mu_p(D_p) \prod_{p|d'} \int_{D_p} u_p(x) d\mu_p
\]
\[= \sum_{n=1}^{N} \prod_{p} u_p(n) - N \cdot \prod_{p} \int_{\mathbb{Z}_p} u_p(x) d\mu_p
\]
is at most \( \frac{c_3}{O} \) with \( C_3 = C_4 = 1 \) and \( M \) arbitrary. The first term of (3.1) is \( O \left( \frac{\log M}{M^{1/2}} N \right) \), where \( c \) and the implied constant depend only on \( C_0, C_1 \) and \( C_2 \). The second term is \( O(M \log M) \). By Lemma 3.2, the third term is no greater than
\[
\sum_{1 \leq d \leq M^{1/2}} \sum_{d' \leq d, \text{ sq-free}} \left( 2c_0^{\omega(d)} \prod_{p|d} c_2 \log N \frac{\log p}{\log p} + \frac{c_1}{1 - p^{-c_2}} \cdot \omega(d) + c_0^{\omega(d)} \right) \ll M^{1/2+\epsilon}.
\]

Set \( M = N^{2/3} \). The result follows. \( \square \)

**Proposition 3.8.** For every \( p \), let \( u_p : \mathbb{Z}_p^2 - p\mathbb{Z}_p^2 \to \mathbb{C} \) be a \((c_0, c_1p^{-c_2})\)-approximable function, where \( c_0 \) is a positive integer and \( c_1, c_2 \) are positive real numbers. Assume that \(|u_p(x,y)| \leq 1 \) 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
\[
\sum_{-N \leq x,y \leq N} \prod_{p} u_p(x,y)
\]
equals
\[
(\#(S \cap [-N,N]^2)) \cdot \prod_{p} \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} u_p(x,y) dxdy + O((\log N) N^{4/3})
\]
\[+ O\{x,y \in [-N,N] : \gcd(x,y) = 1, \exists p > N^{4/3} \text{ s.t. } p^2 | P(x,y)\},
\]
where the implied constants depend only on \( P, c_0, c_1 \) and \( c_2 \).
Proof. We define a soil \((\mathcal{P}, \mathcal{A}, r, f)\) by
\[
\mathcal{P} = \{ p \in \mathbb{Z}^+ : p \text{ prime} \}, \quad \mathcal{A} = \{ 1 \leq x, y \leq N : \gcd(x, y) = 1 \},
\]
\[
r((x, y)) = \{ p \in \mathcal{P} : p^2 | P(x, y) \}, \quad f((x, y), d) = \prod_{p \mid d} u_p(x, y).
\]
Let \(h(d) = \prod_{p \mid d} p^2\). Properties (h1) and (h2) are clear. Lemmas A.3 and A.5 give us property (A1) with
\[
X = N^2 \prod_p \left(1 - \frac{1}{p^2}\right), \quad C_0 \ll |\text{Disc } P|^3, \quad C_1, C_2 \ll \deg P.
\]
Choose the sampling datum in Example 3 with \(n = N\). Proceed as in Prop. 3.7. \(\square\)

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 \(x \mod p\) and \(v_p(P(x))\). Then \(u_p\) is \((c_0, c_1 p^{-\epsilon})\)-approximable, where \(c_0, c_1\) depend only on \(P\), not on \(p\).

Proof. Let \(c_0 = 2 |\text{Disc } P|^3 \deg P, c_1 = |\text{Disc } P|^3 \deg P\). Let \(x_1, \ldots, x_c\) be the solutions to \(P(x) \equiv 0 \pmod{p}\) in \(\mathbb{Z}/p\). Clearly \(c \leq \deg P\). Define
\[
M_{p,j_0,j_1} = \{ x \in \mathbb{Z}_p : v_p(P(x)) = j_0, x \equiv x_{j_1} \pmod{p} \}.
\]
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
\[
\mu_p(M_{p,j_0,j_1}) \leq \mu_p(\{ x \in \mathbb{Z}_p : v_p(P(x)) = j_0 \}) \leq c_1 p^{-j_0}.
\]
Let \(c_2 = 1 / \deg P\). Thus \(c_2 \leq 1/c\). The statement follows. \(\square\)

**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 \(xy^{-1} \pmod{p}\) in \(\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})\) and \(v_p(P(x, y))\). Then \(u_p\) is \((c_0, c_1 p^{-\epsilon})\)-approximable, where \(c_0, c_1\) depend only on \(P\), not on \(p\).

Proof. Same as Lemma 3.9. \(\square\)

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,

\[
(3.11) \quad \frac{1}{N/m} \sum_{\substack{1 \leq n \leq N \\ n \equiv a \mod{m}}} \mu(n) \ll Ne^{-C((\log N)^{2/3}/(\log \log N)^{1/5}}
\]

for \( m \leq (\log N)^A \), where both \( C \) and the implied constant depend only on \( A \). We would like to show that \( \mu(P(n)) \prod_p u_p(n) \) 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

\[
W(\mathcal{E}(n)) = \prod_p W_0,p(\mathcal{E}(n)) \cdot \prod_p \frac{W_p(\mathcal{E}(n))}{W_0,p(\mathcal{E}(n))} = f(n) \cdot \prod_p u_p(n).
\]

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

\[
g(n) \cdot \prod_p u_p(n) = \prod_p u_p,1(n).
\]

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

\[
\lim_{N \to \infty} \frac{1}{N} \sum_{1 \leq x,y \leq N \atop \gcd(x,y) = 1} \mu(P(x,y)) = 0 \quad \text{Chowla’s conjecture}.
\]

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

\[
\sum_{1 \leq x,y \leq N \atop \gcd(x,y) = 1} W(\mathcal{E}(x/y)),
\]

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

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

for every lattice \( L \) with \([\mathbb{Z}^2 : L] \leq (\log N)^A \), 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 $(c_0, c_1 p^{-c_2})$-approximable function, where $c_0$ is a positive integer and $c_1$, $c_2$ are positive real numbers. Assume that $|u_p(x)| \leq 1$ for every $x \in \mathbb{Z}_p$. Assume, furthermore, that $u_p(x) = 1$ unless $p^2 | P(x)$, where $P \in \mathbb{Z}[x]$ is a fixed square-free polynomial.

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

$$\sum_{\substack{1 \leq n \leq N \\text{mod } m}} s(n) = N \cdot \prod_p \sigma_p(\{n \in \mathbb{Z}_p : n \equiv a \text{ mod } p^{v_p(m)}\}) + O\left(\frac{(\epsilon(N)N)}{m}\right)$$

(3.12)

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

$$\frac{1}{N} \sum_{n=1}^{N} s(n) u_p(n) = \prod_p \int_{\mathbb{Z}_p} u_p(x) d\sigma_p + O\left(\epsilon(N) + \frac{1}{\eta(N)^{1/2 - \epsilon'}}\right) + \frac{1}{N} O\{1 \leq x \leq N : \exists p > N^{1/2} \text{ s.t. } p^2 | P(x)\}.$$  

(3.13)

for all $\epsilon' > 0$, where the implied constant depends only on $P$, $c_0$, $c_1$, $c_2$, $\epsilon'$, and the implied constant in 3.12.

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

$$r_{d_1, d_2} \leq N \cdot \sum_{(s_j) \in (\mathbb{Z}^+)^{d_1} - S \in \mathcal{A}} \prod_{p \in d_1} m_p(s_p) + c_0^{#d_1} \epsilon(N) N \prod_{j \in d_1} \mu_j(M_j)$$

$$+ \#S N^{c_0^{#d_1} \epsilon(N)} + (\#S + 1) c_0^{#d_1}$$

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

$$S = \chi_{p \in d_1}\{n \in \mathbb{Z} : 1 \leq n \leq \frac{c_2 \log \eta(N)}{\log p}\}.$$  

Then

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

and

$$r_{d_1, d_2} \ll c_0^{#d_1} \cdot \left(\frac{(\epsilon(N)N)}{h(d_1)} (\deg P)^{#d_1} + \frac{N}{\eta(N)} #d_1 + \frac{N}{\eta(N)} \prod_{p \in d_1} \frac{c_2 \log \eta(N)}{\log p}\right).$$
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
\[ O \left( \epsilon(N)N + \frac{NM^{1/2+\epsilon'}}{\eta(N)^{1-\epsilon'}} \right). \]
The fourth term is
\[
\sum_{p>M} \# \{1 \leq x \leq N : p^2 | P(x) \} = \sum_{M < p \leq N^{1/2}} \# \{1 \leq x \leq N : p^2 | P(x) \} \\
+ \sum_{p > N^{1/2}} \# \{1 \leq x \leq N : p^2 | P(x) \} \\
\ll \sum_{M < p \leq N^{1/2}} N/p^2 \\
+ \# \{1 \leq x \leq N : \exists p > N^{1/2} \text{ s.t. } \exists \sigma \in \sum_{p \leq N^{1/2}} \text{s.t. } p^2 | P(x) \} \\
\leq NM^{-1} \\
+ \# \{1 \leq x \leq N : \exists p > N^{1/2} \text{ s.t. } p^2 | P(x) \}.
\]
Set \( M = \eta(N) \). The result follows. \( \square \)

**Proposition 3.12.** For every \( p \), let \( u_p : \mathbb{Z}_p^2 - p\mathbb{Z}_p^2 \to \mathbb{C} \) be a \((c_0, c_1p^{-c_2})\)-approximable function, where \( c_0 \) is a positive integer and \( c_1, c_2 \) are positive real numbers. Assume that \(|u_p(x, y)| \leq 1 \) 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 \(|s(x, y)| \leq 1 \) for all \( x, y \in \mathbb{Z}, \gcd(x, y) = 1 \). Let \( \sigma_p \) be a measure on \( \mathbb{Z}_p^2 - p\mathbb{Z}_p^2 \) with \( \max_{S \subset \mathbb{Z}_p^2 - p\mathbb{Z}_p^2} |\sigma_p(S) - \mu_p(S)| \leq 1 \), where \( \mu_p \) is the usual measure on \( \mathbb{Z}_p^2 \). Suppose there are \( \epsilon(N), \eta(N) \) with \( 0 \leq \epsilon(N) \leq 1, 1 \leq \eta(N) \leq N \), such that
\[
\sum_{-N \leq x, y \leq N} s(x, y) = N^2 \prod_p \sigma_p(\{(x, y) \in (\mathbb{Z}_p^2 - p\mathbb{Z}_p^2) \cap L_p \}) + O \left( \frac{\epsilon(N)N}{\max_{L \subset \mathbb{Z}_p^2} |L|} \right)
\]
for all lattices \( L \subset \mathbb{Z}^2 \) with \( |\mathbb{Z}_p^2 : L| \ll \eta(N) \), where \( L_p \subset \mathbb{Z}_p^2 \) is the additive subgroup of \( \mathbb{Z}_p^2 \) generated by \( \mathbb{Z}_pL \). Then
\[
\frac{1}{N^2} \sum_{-N \leq x, y \leq N} s(x, y) \prod_p u_p(x, y) = \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} u_p(x, y) d\sigma_p \\
+ O \left( \epsilon(N) + \frac{1}{\eta(N)^{1/2-\epsilon'}} \right) \\
+ \frac{1}{N^2} O \{|-N \leq x, y \leq N : \gcd(x, y) = 1, \exists p > N \text{ s.t. } p^2 | P(x, y) \} \} \} \}
\]
for all $\epsilon' > 0$, where the implied constant depends only on $P$, $c_0$, $c_1$, $c_2$, $\epsilon'$, and the implied constant in (3.14).

Proof. As in Proposition 3.11. Use Prop. 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 $a + m\mathbb{Z}$:

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

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

$$\frac{1}{N}O\{1 \leq x \leq N : \exists p > N^{1/2} \text{ s.t. } p^2 | P(x)\}$$

and

$$\frac{1}{N^2}O\{-N \leq x, y \leq N : \gcd(x, y) = 1, \exists p > N \text{ s.t. } p^2 | P(x, y)\},$$

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 $\hat{h}$ 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

$$H(y) = (H_K(y))^{1/[K:\mathbb{Q}]},$$

$$H_K(y) = \prod_v \max(|y|_v^{n_v}, 1),$$

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
\[
H(x) = H_Q(x) = \max(|x_0|, |x_1|),
\]
\[
h_x((x, y)) = \log(\max(|x_0|, |x_1|)).
\]

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

**Lemma 4.1.** Let \( f \in \Z[x] \) 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 \( P = (x, y) \in E_d(\Q) \). Consider the point \( P' = (x, d^{1/2}y) \) on \( E_1 \). Then \( \hat{h}(P) = \hat{h}(P') \), 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
\[
\hat{h}(P) = \frac{1}{2} \lim_{N \to \infty} 4^{-N}h_x([2^N]P) = \frac{1}{2} \lim_{N \to \infty} 4^{-N}h_x([2^N]P') = \hat{h}(P').
\]
\( \square \)

**Lemma 4.2.** Let \( f \in \Z[x] \) be an irreducible polynomial. Let \( C \) be the curve given by \( C : y^2 = f(x) \). Let \( d \in \Z \) be square-free. Let \( x, y \) be rational numbers, \( y \neq 0 \), such that \( P = (x, d^{1/2}y) \) lies on \( C \). 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
\[
H(y) = \max \left( \frac{|y_0| |d|^{1/2}}{\sqrt{\gcd(d, y_1^2)}}, \frac{|y_1|}{\sqrt{\gcd(d, y_1^2)}} \right)
\]
(4.1)

Write \( a \) for the leading coefficient of \( f \). Let \( p | \gcd(d, y_1^2) \), \( p \nmid a \). Since \( d \) is square-free, \( p^2 \nmid \gcd(d, y_1^2) \). Suppose \( p^2 \nmid y_1 \). Then \( \nu_p(dy_1^2) = -1 \). However, \( dy_1^2 = f(x) \) implies that, if \( \nu_p(x) \geq 0 \), then \( \nu_p(dy_1^2) \geq 0 \), and if \( \nu_p(x) < 0 \), then \( \nu_p(dy_1^2) \leq -3 \). Contradiction. Hence \( p | \gcd(d, y_1^2) \), \( p \nmid a \) 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
\[
H(P) \geq \max \left( \frac{|d|^{1/2}}{\sqrt{\gcd(d, y_1^2)}}, \frac{|y_1|}{\sqrt{\gcd(d, y_1^2)}} \right)
\]
\[
\geq \max \left( \frac{|d|^{1/2}}{\sqrt{\gcd(d, y_1^2)}}, \frac{\gcd(d, y_1^2)^{3/2}}{a^2} \right).
\]
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
\[ h_y(P) = \log H(P) \geq \frac{3}{8} \log |d| - \frac{1}{2} \log |a|. \]
\[ \square \]

**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
\[ \hat{h}(P) \geq \frac{1}{8} \log |d| + C_f, \]
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, \( \hat{h}(P) = \hat{h}(P') \). The difference \(|\hat{h} - h_x|\) is bounded on \( E \). The statement follows from Lemma 4.2. \[ \square \]

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 \( Q(\bar{x}) \geq c_1 \) for all non-zero \( \bar{x} \in \mathbb{Z}^r \). Then there are at most
\[ (1 + 2\sqrt{c_2/c_1})^r \]
values of \( \bar{x} \) for which \( Q(\bar{x}) \leq c_2 \).

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

**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 \( \hat{h}(P) < c_1 \). Then there are at most
\[ O \left( (1 + 2\sqrt{c_2/c_1})^{\text{rank}(E)} \right) \]
points \( P \in E(\mathbb{Q}) \) for which \( \hat{h}(P) < c_2 \). The implied constant is absolute.

**Proof.** The canonical height \( \hat{h} \) is a positive definite quadratic form on the free part \( \mathbb{Z}^{\text{rank}(E)} \) of \( E(\mathbb{Q}) \sim \mathbb{Z}^{\text{rank}(E)} \times T \). A classical theorem of Mazur’s [Maz] states that the cardinality of \( T \) is at most 16. Apply Lemma 4.3. \[ \square \]

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 \( f(x) = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}[x] \) be an irreducible polynomial of degree 4. For every square-free \( d \in \mathbb{Z} \), consider the curve
\[
C_d : dy^2 = f(x).
\]
If there is a rational point \((r, s)\) on \(C_d\), then there is a birational map from \(C_d\) to the elliptic curve
\[
E_d : dy^2 = x^3 + a_2 x^2 + (a_1 a_3 - 4a_0 a_4)x - (4a_0 a_2 a_4 - a_1^2 a_4 - a_0 a_3^2).
\]
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:
\[
x_1 = x - r, \quad y_1 = y
\]
satisfy
\[
y_1^2 = \frac{1}{d} \left( \frac{1}{4!} f^{(4)}(r) x_1^4 + \frac{1}{3!} f^{(3)}(r) x_1^3 + \frac{1}{2!} f''(r) x_1^2 + \frac{1}{1!} f'(r) x_1 + f(r) \right).
\]
We now apply the standard map for putting quartics in Weierstrass form:
\[
x_2 = \frac{2s(y_1 + s) + f'(r)x_1/d}{x_1^2},
\]
\[
y_2 = \frac{4s^2(y_1 + s) + 2s(f'(r)x_1/d + f''(r)x_1^2/(2d)) - (f'(r)/d)^2 x_1^2/(2s))}{x_1^3}
\]
satisfy
\[
y_2^2 + A_1 x_2 y_2 + A_3 y_2 = x_2^3 + A_2 x_2^2 + A_4 x_2 + A_6
\]
with
\[
A_1 = \frac{1}{d} f'(r)/s, \quad A_2 = \frac{1}{d} (f''(r)/2 - (f'(r))^2/(4f(r))),
\]
\[
A_3 = \frac{2s}{d} f^{(3)}(r)/3!, \quad A_4 = -\frac{1}{d^2} \cdot 4f(r) \cdot \frac{1}{4}! f^{(4)}(r),
\]
\[
A_6 = A_2 A_4.
\]
To take (4.4) to \(E_d\), we apply a linear change of variables:
\[
x_3 = d x_2 + r(a_3 + 2a_4 r), \quad y_2 = \frac{d}{2} (2y_2 + a_1 x_2 + a_3)
\]
satisfy
\[
dy_3^2 = x_3^3 + a_2 x_3^2 + (a_1 a_3 - 4a_0 a_4)x_3 - (4a_0 a_2 a_4 - a_1^2 a_4 - a_3 a_0^2).
\]
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
\[
dy^2 = a_4 x^4 + a_3 x^3 z + a_2 x^2 z^2 + a_1 x z^3 + a_0 z^4.
\]
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
Let \( r = x_0/z_0, \ s = y_0/z_0^2 \) and define a map \( \phi_{r,s} \) from \( C_d \) to \( E_d \) as above. Now let \( x, y, z \in \mathbb{Z}, \ |x|, |z| \leq N, \ z_0 \neq 0 \), 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 \( a_0, a_1, \cdots, a_4 \). In other words,

\begin{equation}
(4.6) \quad h_x(P) \leq 7 \log N + C,
\end{equation}

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 \( E_d \).

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 \( \hat{h}_{E_1}(P) \) be the canonical height of \( P \) as a point of \( E_1 \). Then

\[ |\hat{h}_{E_1}(P) - \frac{1}{2} h_x(P)| \leq C', \]

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

\[ |\hat{h}_{E_d}(P) - \frac{1}{2} h_x(P)| \leq C'. \]

Then, by (4.6),

\[ \hat{h}_{E_d}(P) \leq \frac{7}{2} \log N + (C/2 + C'). \]

We have proven

\textbf{Lemma 4.6.} Let \( f(x, z) = a_4 x^4 + a_3 x^3 z + a_2 x^2 z^2 + a_1 x z^3 + a_0 z^4 \in \mathbb{Z}[x, z] \) 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 \(|x|, |z| \leq N, \gcd(x, z) = 1 \). Let \( S_{d,2} \) be the set of all rational points \( P \) on

\begin{equation}
(4.7) \quad E_d : dy^2 = x^3 + a_2 x^2 + (a_1 a_3 - 4 a_0 a_4) x - (4 a_0 a_2 a_4 - a_1^2 a_4 - a_0 a_3^2)
\end{equation}

with canonical height

\[ \hat{h}(P) \leq \frac{7}{2} \log N + C_f. \]

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
\[
\#S_d \ll \begin{cases} 
(1 + 2\sqrt{\left(\frac{7}{2}\log N + C_{f,1}\right)/\left(\frac{1}{8}\log |d| + C_{f,2}\right)})^{\text{rank}(E_d)} & \text{if } |d| \geq C_{f,4}, \\
(1 + 2C_{f,3}\sqrt{\frac{7}{2}\log N + C_{f,1}})^{\text{rank}(E_d)} & \text{if } |d| < C_{f,4},
\end{cases}
\]
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 4.3 and Lemma 4.6. If \(|d| > C_{f,4}\), apply Corollary 4.3, Corollary 4.5, and Lemma 4.6. \( \square \)

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
\[
\omega_K(d) = \sum_{\substack{p \in \mathcal{O}_K \cap \mathbb{Z} \mid p \nmid d}} 1.
\]

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 \( \alpha \) 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
\[
\text{rank}(E_d) = C_f + \omega_K(d) - \omega(d),
\]
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 \( f_d(x) = a_3x^3 + da_2x^2 + \beta^2a_1x + \beta^2a_0 \). Then \( da \) is a root of \( f_d(x) = 0 \). Clearly \( \mathbb{Q}(da) = \mathbb{Q}(\alpha) \). 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. \( \square \)

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

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

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

\[
S_\alpha(X) \sim C_{K,\alpha} X (\log X)^{\frac{1}{2} + 2\alpha - 1} \quad \text{if } K/Q \text{ is Galois},
\]

\[
S_\alpha(X) \sim C_{K,\alpha} X (\log X)^{\frac{1}{2} + 2\alpha + \frac{1}{2} - 1} \quad \text{if } K/Q \text{ is not Galois},
\]

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

**Proof.** Suppose \( K/Q \) is Galois. Then, for \( \Re s > 1 \),

\[
\zeta_{K/Q}(s) = \prod_{p \in I_K} \frac{1}{1 - (Np)^{-s}} = \prod_{p \text{ ramified}} \frac{1}{1 - p^{-s}} \prod_{p \text{ unsplit \& unram.}} \frac{1}{1 - p^{-3s}} \prod_{p \text{ split}} \frac{1}{1 - p^{-3s}}.
\]

Hence

\[
\prod_{p \text{ split}} (1 + \beta p^{-s}) = L_1(s)(\zeta_{K/Q}(s))^{\beta/3},
\]

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

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

it follows that

\[
\sum_n R(\alpha, n) = L_1(s)(\zeta_{K/Q}(s))^{22\alpha/3}.
\]

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

\[
\frac{1}{X} \sum_{n \leq X} R(\alpha, n) \sim C_{K,\alpha} (\log X)^{\frac{1}{2} + 2\alpha - 1}
\]

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

Now suppose that \( K/Q \) is not Galois. Denote the splitting type of a prime \( p \) in \( K/Q \) by \( p = p_1 p_2, p = p_1 p_2 p_3, p = p_1^2 p_2, \) etc. Let \( L/Q \) be the Galois closure of \( K/Q \). By Lemma 4.19

\[
\zeta_{K/Q}(s) = \prod_{p \in I_K} \frac{1}{1 - (Np)^{-s}} = L_2(s) \prod_{p = p_1 p_2} \frac{1}{1 - p^{-s}} \prod_{p = p_1 p_2 p_3} \frac{1}{1 - p^{-3s}},
\]

\[
\zeta_{L/Q}(s) = \prod_{p \in I_L} \frac{1}{1 - (Np)^{-s}} = L_3(s) \prod_{p = p_1 p_2 p_3} \frac{1}{1 - p^{-6s}},
\]

By a Tauberian theorem, we can conclude that

\[
\sum_{n \leq X} R(\alpha, n) \sim C_{K,\alpha} (\log X)^{\frac{1}{2} + 2\alpha - 1}
\]

for some positive constant \( C_{K,\alpha} > 0 \).
where \( L_2(s) \) and \( L_3(s) \) are continuous, non-zero and bounded on \( \{ s : \Re s > \frac{1}{2} \} \). Thus
\[
\sum_n R(\alpha, n)n^{-s} = \prod_{\mathfrak{p}=\mathfrak{p}_1\mathfrak{p}_2} (1 + 2^\alpha \mathfrak{p}^{-s}) \prod_{\mathfrak{p}=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} (1 + 2^{2\alpha} \mathfrak{p}^{-s})
= L_4(s) \zeta_{K/Q}(s)^{2\alpha} \zeta_{L/Q}^{-\frac{1}{2}2^{2\alpha} + \frac{1}{6}2^{2\alpha}}.
\]

Since \( \zeta_{K/Q} \) and \( \zeta_{L/Q} \) both have a pole of order 1 at \( s = 1 \), we can apply a Tauberian theorem as before, obtaining
\[
\frac{1}{X} \sum_{n \leq X} R(\alpha, n) \sim C_{K,\alpha}(\log X)^{\frac{1}{2}\alpha + \frac{1}{6}2^{2\alpha} - 1}.
\]
\( \square \)

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 \((x, y) \in \mathbb{Z}^2, |x|, |z| \leq N, \gcd(x, z) = 1, \) such that
\[
(4.12) \quad p^2 \mid f(x, z).
\]

**Proof.** If \( N \) is large enough, then \( p \) does not divide the discriminant of \( f \). Hence
\[
(4.13) \quad f(r, 1) \equiv 0 \mod p^2
\]
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 \((x, y) \in \mathbb{Z}^2\) to \((4.12)\) with \( x, y \) 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
\[
0 \leq |x_0|, |x_1|, |z_0|, |z_1| \leq N,
\]
\[
\gcd(x_0, z_0) = \gcd(x_1, z_1) = 1,
\]
\[
x_0/z_0 \equiv r \equiv x_1/z_1 \mod p^2.
\]
Then
\[
x_0z_1 - x_1z_0 \equiv 0 \mod p^2.
\]
Since \( 0 \leq x_j, z_j \leq N \) and \( p > N \), we have that
\[
-p^2 < x_0z_1 - x_1z_0 < p^2,
\]
and thus \( x_0z_1 - x_1z_0 \) 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 \( \text{sgn}(x_0) = \text{sgn}(x_1) \), it follows that \((x_0, z_0) = (x_1, z_1)\). \( \square \)

**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

\[
\delta(N) = \{x, z \in \mathbb{Z}^2 : |x|, |z| \leq N, \gcd(x, z) = 1, \exists p > N \text{ s.t. } p^2 | f(x, y) \}.
\]

Then

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

where \( A \) and the implied constant depend only on \( f \).

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

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

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

Let \( M \leq N^3 \). By Lemma 4.11

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

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

\[
\sum_{0 < |d| \leq M} S(d),
\]

where we write

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

Let \( C_{f,1}, C_{f,2}, C_{f,3}, C_{f,4} \) be as in Proposition 4.7. Let \( K, C_f, \omega \) and \( \omega_K \) 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 \( C_1 = \max_{0 < d < C_{f,4}} \text{rank}(E_d) \), \( C_2 \) and the implied constant depend only on \( f \). Let \( \epsilon \) be a small positive real number. By Proposition 4.7 and Lemma 4.8

\[
\sum_{C_{f,4} \leq |d| < N^\epsilon} S(d) \ll \sum_{C_{f,4} \leq |d| < N^\epsilon} \left( 1 + 2 \sqrt{\frac{7}{2} \log N + C_{f,1}} \right)^{\text{rank}(E_d)} 
\]

\[
\ll \sum_{C_{f,4} \leq |d| < N^\epsilon} \left( 1 + 2 \sqrt{\frac{7}{2} \log N + C_{f,1}} \right)^{C_{f,5} + \omega_K(d) - \omega(d)}.
\]

We have the following crude bounds:

\[
(4.14) \quad \omega(d) \leq \frac{\log |d|}{\log \log |d|}, \quad \omega_K(d) \leq 3\omega(d).
\]
Hence
\[
\sum_{C_f,\delta \leq |d| < N^\varepsilon} S(d) \ll \sum_{C_f,\delta \leq |d| < N^\varepsilon} (\log N)^{C_f,\delta + 2\log d/\log \log d} \leq N^\varepsilon (\log N)^{C_1} (\log N)^{2\varepsilon \log N/\log \log N} \leq (\log N)^{C_1} N^{3\varepsilon},
\]
where \(C\) depends only on \(f\) and \(\varepsilon\). For any \(|d| > N^\varepsilon\), Proposition 4.13 and Lemma 4.10 give us
\[
S(d) \ll \left( 1 + 2 \sqrt{\frac{7}{2} \log N + C_{f,1}} \right) / \left( \frac{1}{8} \varepsilon \log N + C_{f,2} \right) \ll (12\varepsilon^{-1/2})^{C_{f,\delta} + \omega_K(d) - \omega(d)} \leq 2^{C_{f,\delta} + \omega_K(d) - C_{2\omega_K(d)}},
\]
where \(C_2\) depends only on \(f\) and \(\varepsilon\). By Lemma 4.10 we can conclude that
\[
\sum_{N^\varepsilon < |d| \leq M} S(d) \ll \sum_{d=1}^{M} 2^{C_{2\omega_K(d) - C_{2\omega_K(d)}}} \ll C_3 M (\log N)^{C_4},
\]
where \(C_3\) and \(C_4\) depend only on \(f\) and \(\varepsilon\). Set \(M = N^{4/3}, \varepsilon = 1/4\). \(\square\)

4.5. Homogeneous cubics.

**Proposition 4.13.** Let \(f \in \mathbb{Z}[x, z]\) be a homogeneous irreducible polynomial of degree 3. Let
\[
\delta(N) = \{x, z \in \mathbb{Z}^2 : |x|, |z| \leq N, \gcd(x, z) = 1, \exists p > N \text{ s.t. } p^2 \mid f(x, y)\}.
\]
Then
\[
\delta(N) \ll N^{4/3} (\log N)^A,
\]
where \(A\) and the implied constant depend only on \(f\).

**Proof.** Write \(A = \max_{|x|, |z| \leq N} f(x, z)\). Clearly \(A \ll N^4\). We can write
\[
\delta(N) \leq \sum_{0 < |d| \leq M} \# \{x, y, z \in \mathbb{Z}^2, |x|, |z| \leq N, \gcd(x, z) = 1 : dy^2 = f(x, z)\} + \sum_{N < p \leq \sqrt{A/M}} \# \{x, z \in \mathbb{Z}^2, |x|, |z| \leq N, \gcd(x, z) = 1 : p^2 \mid f(x, z)\}.
\]
Let \(M \leq N^2\). 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
\[
(4.15) \quad d'y'^2 = f(x', 1),
\]
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 \(d \leq M\), then \(|d'| = |dz| \leq MN\). The height \(h_x(P)\) of the point \(P = (x/z, y/z^2)\) is at most \(N\). It follows by Lemma 4.14 that \(h(P) \leq N + C_f\), where \(C_f\) is a constant depending only on \(f\). By Corollaries 4.3 and 4.3, there are at most
\[
O \left( (1 + 2 \sqrt{(\log N + C_f')/(\log |d| + C_f)})^{\text{rank}(E_d)} \right)
\]
rational points $P$ of height $\hat{h}(P) \leq N + C_f$. We proceed as in Proposition 4.12 and obtain that
\[ \sum_{0 <|d| \leq M} \# \{ x, y, z \in \mathbb{Z}^3, |x|, |z| \leq N, \gcd(x, z) = 1 : dy^2 = f(x, z) \} \]
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 $M < N^{\deg f}$, $\epsilon > 0$,
\[ \sum_{d = 1}^{M} \# \{ x, y, z \in \mathbb{Z}^3, |x|, |z| \leq N, \gcd(x, z) = 1 : dy^2 = f(x, z) \} \]
is at most a constant times $N^{(18 - \frac{1}{2}\beta^2)/(10 - \beta) + \epsilon}$, where $\beta = (\log M)/(\log N)$. The implied constant depends only on $f$ and $\epsilon$.

**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
\[ \delta(N) = \{ x, z \in \mathbb{Z}^2 : |x|, |z| \leq N, \gcd(x, z) = 1, \exists p > N \text{ s.t. } p^2 | P(x, y) \}. \]
Then, for any $\epsilon > 0$,
\[ \delta(N) \ll N^{(5 + \sqrt{113})/8 + \epsilon} \]
where the implied constant depends only on $f$ and $\epsilon$.

**Proof.** Let $A = \max_{|x|, |z| \leq N} f(x, z)$. Clearly $A \ll N^{\deg(f)}$. We can write
\begin{align*}
\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 | f(x, z) \}.
\end{align*}
By Lemmas 4.14 and 4.11
\[ \delta(N) \ll N^{(18 - \frac{1}{2}\beta^2)/(10 - \beta) + \epsilon} + \frac{1}{\log N} \sqrt{N^{\deg(f)-\beta}}, \]
where $\beta = (\log M)/(\log N)$. Set $\beta = (15 - \sqrt{113})/4$. □

4.7. Quasiorthogonalities, kissing numbers and cubics.

**Lemma 4.16.** 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
\[ \hat{h}(P + P') \leq 3 \max(\hat{h}(P), \hat{h}(P')) + C_f, \]
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,

\[
x'' = \frac{d(y_2 - y_1)^2}{a_3(x_2 - x_1)^2} - \frac{a_2}{a_3} - x_1 - x_2
\]

\[
= \frac{d(y_2 - y_1)^2 - a_2(x_2 - x_1)^2 - a_3(x_2 - x_1)^2(x_1 + x_2)}{a_3(x_2 - x_1)^2}.
\]

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

\[
h_x(P) = \log(\max(|\num(x'')|, |\den(x'')|))
\]

\[
\leq 3 \max(\log |x|, \log |x'|) + \log A
\]

\[
\leq 3 \max(h_x(P), h_x(P')) + \log A.
\]

By Lemma 4.1 the difference \(|\hat{h} - h_x|\) 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 \( \mathbb{R}^{\text{rank}(E_d)} \) 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 \( L(P) \in \mathbb{R}^{\text{rank}(E_d)} \) whose Euclidean norm \( |L(P)| \) satisfies

\[|L(P)|^2 = \hat{h}(P) = \log x + O(1),\]

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

\[(4.16) \quad N^{1-\epsilon} \leq x \leq N\]

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

\[(1 - \epsilon) \log N + O(1) \leq |L(P)|^2 \leq \log N + O(1)\].

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

\[|L(P) + L(P')|^2 = |L(P + P')|^2 \leq 3 \max(|L(P)|^2, |L(P')|^2) + O(1)\].
Therefore, the inner product $L(P) \cdot L(P')$ satisfies

$$L(P) \cdot L(P') = \frac{1}{2}(|L(P) + L(P')|^2 - (|L(P)|^2 + |L(P')|^2))$$

$$\leq \frac{1}{2}(3 \max(|L(P)|^2, |L(P')|^2) + O(1) - (|L(P)|^2 + |L(P')|^2))$$

$$\leq \frac{1}{2}((1 + \epsilon) \log(N) + O(1))$$

$$\leq \frac{1}{2}(1 + \epsilon) \frac{O((\log N)^{-1})}{(1 - \epsilon)^2} |L(P)||L(P')|.$$ 

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

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

Let $L$ be a linear map taking $E(\mathbb{Q})$ to $\mathbb{R}^{\text{rank}(E_d)}$ and the square of the Euclidean norm back to the canonical height $\hat{h}$. Then, for any distinct points $P, P' \in L(S) \subset \mathbb{R}^{\text{rank}(E_d)}$ with the angle $\theta$ between $P$ and $P'$ is at least

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

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 $\theta$. Kabatiansky and Levenshtein ([KL]; v.d. also [CS], (9.6)) show that, for $n$ large enough,

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

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

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

Then

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

where

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

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 
\[ \delta(N) = \{1 \leq x \leq N : \exists p > N^{1/2} \text{ s.t. } p^2 | f(x)\}. \]

Then 
\[
\delta(N) \ll N(\log N)^{-\beta},
\]
where 
\[ \beta = 1 - \frac{1}{9} 2^{2\alpha} = 0.8061 \ldots \]
if the discriminant of \( f \) is a square,
\[ \beta = 1 - \frac{1}{6} 2^{\alpha} - \frac{1}{18} 2^{2\alpha} = 0.6829 \ldots \]
if the discriminant of \( f \) is not a square, and \( \alpha \) is as in (4.18). The implied constant in (4.19) depends only on \( f \).

**Proof.** Let \( A = \max_{1 \leq x \leq N} f(x) \). Clearly \( A \ll N^3 \). We can write
\[
\delta(N) \leq \sum_{N^{1/2} < p < \sqrt{A/M}} \#\{1 \leq x \leq N : p^2 | f(x)\} 
+ \#\{1 \leq x \leq N^{1-\epsilon} : \exists p > N^{1/2} \text{ s.t. } p^2 | f(x)\} 
+ \sum_{1 \leq |d| \leq M} \#\{x, y \in \mathbb{Z}^2 : N^{1-\epsilon} \leq x \leq N, dy^2 = f(x)\}.
\]
Let \( M \leq N^2 \). 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 \( N^{1-\epsilon} \). It remains to bound 
\[
\sum_{1 \leq |d| \leq M} B(d),
\]
where 
\[ B(d) = \#\{x, y \in \mathbb{Z}^2 : N^{1-\epsilon} \leq x \leq N, dy^2 = f(x)\}. \]

By Lemma 4.10 Corollary 4.18 and the remark before 4.18 
\[ B(d) \ll R(\alpha + O(\epsilon + (\log N)^{-1}), d), \]
where \( K \) is as in Lemma 4.8 and \( \alpha \) is as in Corollary 4.18 and \( R(\alpha, d) \) is as in 4.8. Thanks to (4.12), we can omit the term \( O((\log N)^{-1}) \) from the exponent. Hence it remains to estimate 
\[ S(M) = \sum_{1 \leq d \leq M} R(\alpha + O(\epsilon + (\log N)^{-1}), d). \]

By Lemma 4.10
\[ S(M) \ll M(\log M)^{\frac{1}{2} 2^{(\alpha + O(\epsilon))^{-1}}} \text{ if } K/\mathbb{Q} \text{ is Galois}, \]
\[ S(M) \ll M(\log M)^{\frac{1}{2} 2^{\alpha + O(\epsilon)} + \frac{1}{2} 2^{(\alpha + O(\epsilon))^{-1}}} \text{ if } K/\mathbb{Q} \text{ is not Galois}. \]
Set
\[ M = N(\log N)^{-\frac{3}{2}} \text{ if } K/\mathbb{Q} \text{ is Galois} \]
\[ M = N(\log N)^{-\frac{3}{2}} \text{ if } K/\mathbb{Q} \text{ is not Galois} \]

Let \( \epsilon = (\log \log M)^{-1} \). 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 \( C : y^2 = f(x) \), \( \deg(f) \geq 5 \), 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 \( f \). 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 \( \mu \) commutes with field extensions \( K \to K' \):
\[
\begin{array}{ccc}
J(K) & \to & A_K^*/K^*(A_K^*)^2 \\
\downarrow & & \downarrow \\
J(K') & \to & A_{K'}^*/K'^*(A_{K'}^*)^2
\end{array}
\]
(4.20)

Proof. See [Ca], p. 30, for the statement on the image and kernel of \( \mu \). The commutativity of (4.20) follows from the construction of \( \mu \) 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 \( p \)-adic field \( K \) whose residue field has odd characteristic. Suppose \( C : y^2 = f(x) \) has good reduction. Let \( \mu \) 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 \( \mu \). Then \( v_{K_j}(x_j) \mod 2 \) is independent of \( j \).

Proof. Let \( k \) be the residue field of \( K \), \( \bar{K} \) the maximal unramified extension of \( K \), and \( \bar{k} \) the algebraic closure of \( k \). Let \( J_1(\bar{K}) \) be the kernel of the residue map \( J(\bar{K}) \to J(\bar{k}) \). We have an exact sequence
\[ 0 \to J_1(\bar{K}) \to J(\bar{K}) \to J(\bar{k}) \to 0, \]
from which we obtain
\[ J_1(\bar{k})/2J_1(\bar{k}) \to J(\bar{k})/2J(\bar{k}) \to J(\bar{k})/2J(\bar{k}) \to 0. \]

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

By virtue of the commutative diagram
\[ \begin{array}{ccc} J(K)/2J(K) & \xrightarrow{\mu} & A_{K^*}^*/K^*(A_{K^*}^*)^2 \\ \downarrow & & \downarrow \\ J(\bar{k})/2J(\bar{k}) = \{ e \} & \xrightarrow{\mu} & A_{K^*}/\bar{K}^*(A_{\bar{K}}^*)^2, \end{array} \]
the image of \( \mu(J(K)/2J(K)) \) lies in \( A_{K^*}^* \cap \bar{K}^*(A_{\bar{K}}^*)^2 \). Since, for every index \( j \), the extensions \( \bar{K}_j/K \) and \( \bar{K}_j/\bar{K} \) are unramified, we can write, for any \( r \in \bar{K}^* \), \( s \in A_{\bar{K}}^* \) with \( rs^2 \in A_{\bar{K}}^* \),
\[ v_{\bar{K}_j}(rs^2) = v_{\bar{K}_j}(s^2) = v_{\bar{K}_j}(r) + 2v_{\bar{K}_j}(s) = v_{\bar{K}}(r) + 2v_{\bar{K}}(s). \]
The statement follows. \( \square \)

**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
\[ \text{rank}(C_d) \leq \kappa_f + \sum_{p|d} (n_p - m_p), \]
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 \( \kappa_f \) 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 \( (x) = rs^2 \) for some \( r \in \mathbb{Q}, s \in I_L \). Clearly
\[ \text{rank}(H) \leq 5 + \text{rank}(h_L/h_L^2), \]
where $h_L$ is the class group of $L$. Hence the rank of the kernel of the composition
\[ c : J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q}) \xrightarrow{\mu} A_Q^*/Q_Q^*(A_Q^*)^2 \rightarrow \prod_{\nu}(A_{Q_{\nu}}^*/Q_{Q_{\nu}}^*(A_{Q_{\nu}}^*)^2)/U_{A_{Q_{\nu}}} \]
is at most $6 + \text{rank}(h_L/h_L^2)$. We have a commutative diagram
\[
\begin{array}{ccc}
J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q}) & \xrightarrow{c} & \prod_{\nu}(A_{Q_{\nu}}^*/Q_{Q_{\nu}}^*(A_{Q_{\nu}}^*)^2)/U_{A_{Q_{\nu}}} \\
\downarrow & & \downarrow \\
J_{C_d}(\mathbb{Q}_L)/2J_{C_d}(\mathbb{Q}_L) & \xrightarrow{\mu} & (A_{Q_{\nu}}^*/Q_{Q_{\nu}}^*(A_{Q_{\nu}}^*)^2)/U_{A_{Q_{\nu}}}.
\end{array}
\]
By Lemma 4.21, the bottom row has trivial image when $\nu \neq 2, \infty$ and $C_d$ has good reduction at $\nu$. Thus
\[
\text{rank}(J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q})) \leq 6 + \text{rank}(h_L/h_L^2) + \sum_{\nu=\infty,2 \text{ or }L \text{ ramifies at } \nu \text{ or }C_1 \text{ has bad red. at } \nu} \text{rank}((A_{Q_{\nu}}^*/Q_{Q_{\nu}}^*(A_{Q_{\nu}}^*)^2)/U_{A_{Q_{\nu}}}) + \sum_{p \mid d} \text{rank}(\mu(J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q}))\text{.})
\]
By Lemma 4.20, $\mu(J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q}))$ is contained in the intersection of the kernel of $N_{A_Q/\mathbb{Q}}$ and $(A_{Q_{\nu}}^*/Q_{Q_{\nu}}^*(A_{Q_{\nu}}^*)^2)/U_{A_{Q_{\nu}}}$. Hence the image of
\[
\mu(J_{C_d}(\mathbb{Q}_L)/2J_{C_d}(\mathbb{Q}_L))
\]
under the natural injection
\[
(A_{Q_{\nu}}^*/Q_{Q_{\nu}}^*(A_{Q_{\nu}}^*)^2)/U_{A_{Q_{\nu}}} \rightarrow (\oplus_{p \mid d} \mathbb{Z}/2\mathbb{Z})/(1, \ldots, 1)
\]
consists of cosets $(x_p)_{p \mid d} \in \oplus_{p \mid d} \mathbb{Z}/2\mathbb{Z}$ with $\sum_{p \mid d} f_p x_p$ 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
\[
\text{rank}(J_{C_d}(\mathbb{Q})) \leq \text{rank}(J_{C_d}(\mathbb{Q})/2J_{C_d}(\mathbb{Q})) \leq 6 + \text{rank}(h_L/h_L^2) + \sum_{\nu=\infty,2 \text{ or }L \text{ ramifies at } \nu \text{ or }C_1 \text{ has bad red. at } \nu} \text{rank}((A_{Q_{\nu}}^*/Q_{Q_{\nu}}^*(A_{Q_{\nu}}^*)^2)/U_{A_{Q_{\nu}}}) + \sum_{p \mid d} (n_p - m_p).
\]

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

\textbf{Lemma 4.23.} Let $K/\mathbb{Q}$ be a Galois number field. Let $\langle \gamma \rangle$ be a conjugacy class in $G = \text{Gal}(K/\mathbb{Q})$. Then, for $\Re(s) > 1$,
\[
\prod_{p} (1 - p^{-s})^{-1} = L_0(s) \prod_{\chi} L_{\chi}(s)^{\overline{\langle \gamma \rangle}} \# \langle \gamma \rangle / \# G,
\]
where $\langle \phi \rangle$ is the conjugacy class of $\phi$ in $G$.
where

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

**Proof.** For every character $\chi$ of $G$, the $L$-function $L_\chi$ is of the form

$$L_\chi(s) = \frac{1}{\prod_p (1 - \chi(Frob_p)p^{-s})},$$

where $L_0(s)$ is some function holomorphic and bounded for $\Re s \geq 1/2 + \epsilon$. By the orthogonality of the characters of $G$, we have that $\sum_\chi \chi(Frob_p)\chi(\gamma)$ is $|G|$ for $\langle Frob_p \rangle = \langle \gamma \rangle$, and 0 otherwise. \qed

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

$$\sum_{d \leq X} \prod_{p|d} g(Frob_p) = C_{K,g}X(\log X)^{-1+\frac{1}{\#G}\sum_{\gamma \in \mathcal{C}} g(\gamma)},$$

where $G = \text{Gal}(K/\mathbb{Q})$, $C_{K,g}$ 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

$$\sum_{n} \prod_{p|d} g(Frob_p)n^{-s} = \prod_{\langle \gamma \rangle} \prod_p (1 + g(\gamma)p^{-s} + g(\gamma)p^{-2s} + \cdots),$$

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

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

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

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

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

Let $K/\mathbb{Q}$ be a number field; let $K'/\mathbb{Q}$ be its Galois closure. We can see $\text{Gal}(K'/\mathbb{Q})$ as a transitive permutation group on $\{1, 2, \ldots, \deg(K'/\mathbb{Q})\}$. Since every permutation of $\{1, 2, \ldots, n\}$ is a product of disjoint cycles, we may speak of the cycles of a map $\gamma \in \text{Gal}(K'/\mathbb{Q})$. We write $G_1(K'/\mathbb{Q})$ for the set of all $\gamma \in \text{Gal}(K'/\mathbb{Q})$ fixing at least one point in $\{1, 2, \ldots, \deg(K, \mathbb{Q})\}$

**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 $\alpha$ be a positive real number. Write $K'$ for the splitting field of $f$. Choose
\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
Gal(K'/Q) & \delta & for \(\alpha = 0.4014\ldots\) \\
\hline
C(6) & \frac{1}{4}\alpha & 0.5072\ldots \\
D_6(6) & \frac{1}{2}\alpha & 0.5072\ldots \\
D(6) & \frac{1}{2}\alpha + \frac{1}{12}\alpha & 0.6897\ldots \\
A_4(6) & \frac{1}{2}\alpha + \frac{1}{12}\alpha & 0.6897\ldots \\
F_{18}(6) & \frac{1}{2}\alpha + \frac{18}{2}\alpha & 0.5567\ldots \\
2A_4(6) & \frac{1}{8}\alpha + \frac{1}{8}\alpha + \frac{1}{24}\alpha & 0.6328\ldots \\
S_4(6d) & \frac{3}{8}\alpha + \frac{1}{24}\alpha & 0.7809\ldots \\
S_4(6c) & \frac{1}{2}\alpha + \frac{1}{2}\alpha + \frac{1}{24}\alpha & 0.6750\ldots \\
F_{18}(6) : 2 & \frac{1}{3}\alpha + \frac{1}{3}2\alpha + \frac{1}{24}\alpha & 0.7145\ldots \\
F_{36}(6) & \frac{1}{2}\alpha + \frac{1}{36}\alpha + \frac{1}{24}\alpha & 0.7145\ldots \\
2S_4(6) & \frac{1}{8}\alpha + \frac{1}{16}\alpha + \frac{1}{48}\alpha + \frac{1}{48}\alpha & 0.6996\ldots \\
L(6) & \frac{2}{5} + \frac{1}{2}\alpha + \frac{1}{60}\alpha & 0.8868\ldots \\
F_{36}(6) : 2 & \frac{6}{5}\alpha + \frac{13}{2}\alpha + \frac{1}{24}\alpha + \frac{1}{24}\alpha & 0.7693\ldots \\
L(6) : 2 & \frac{1}{5} + \frac{4}{2}\alpha + \frac{1}{2}\alpha + \frac{1}{24}\alpha & 0.7736\ldots \\
A_6 & \frac{7}{8}\alpha + \frac{1}{2}\alpha + \frac{1}{36}\alpha + \frac{1}{36}\alpha & 0.8203\ldots \\
S_6 & \frac{1}{5} + \frac{7}{21}\alpha + \frac{1}{14}\alpha + \frac{1}{48}\alpha + \frac{1}{48}\alpha & 0.8434\ldots \\
\hline
\end{tabular}
\caption{Galois groups and corresponding averages}
\end{table}

a root \(x_0\) of \(f(x) = 0\). Let \(K = \mathbb{Q}(x_0)\). Let \(R(\alpha, d) = 2^{\alpha \text{rank}(C_d)}\) if no \(p|d\) is unsplit in \(K/\mathbb{Q}\). Let \(R(\alpha, d) = 0\) otherwise. Then

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

where

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

\(n_\gamma\) is the number of cycles of \(\gamma\), and the implied constant in (4.21) depends only on \(K\) and \(\alpha\); the dependence on \(\alpha\) is continuous.

\textbf{Proof.} Immediate from Proposition \ref{prop:4.22} and Corollary \ref{cor:4.24} \hfill \Box

Figure \ref{figure1} gives the value of \(\delta\) in terms of \(\alpha\) and \(\text{Gal}(K'/\mathbb{Q})\). The numerical value of \(\delta\) for \(\alpha = 0.4014\ldots\) is given in the rightmost column. The table was computed by means of the finite-group package GAP \cite{GAP4} running on a GNU/Linux box. The sixteen transitive permutation groups on \(\{1, \ldots, 6\}\) have been labelled as in \cite{CHM}.

\subsection{4.10. Rational points and ranks of Jacobians.}

\textbf{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

\[(4.22) \quad \phi_{d,c} : C_d(K) \xrightarrow{(x,y) \to (x,y\sqrt{d})} C \xrightarrow{P \to \text{Cl}(P)-c} J_C\]

generates an abelian group of rank at most \(\text{rank}(J_{C_d}(K)) + 1\).
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 \(P \mapsto \text{Cl}(P) - t_d^*c\). 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 \(C_d(K)\) under the composition

\[
C_d(K) \xrightarrow{(x, y) \mapsto (x, y\sqrt{d})} C \xrightarrow{P \mapsto \text{Cl}(P) - t_d^*c} J_{C_d}
\]

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

\[
C_d(K) \xrightarrow{(x, y) \mapsto (x, y\sqrt{d})} C \xrightarrow{P \mapsto \text{Cl}(P) - (t_d^{-1})^*c} J_{C_d}
\]

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

**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 \(h_\delta\) be the height function on \(J \times J\) induced by the theta divisor; let \(P \mapsto \text{Cl}(P) - c_0\) 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

\[
\langle P_1, P_2 \rangle = -h_\delta(P_1, P_2), \quad |P| = \sqrt{\langle P, P \rangle}.
\]

Then, for any \(P_1, P_2 \in C(K)\), \(P_1 \neq P_2\),

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

Notice moreover that

\[
\langle P, P \rangle = 2gh_{c_0}(P) + O(1)
\]

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.) \(\square\)

**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 \(\phi_{d,c_0}\) be as in (4.23). Then there is a constant \(\kappa_f\) such that, if \(d\) is a square-free integer \(d\) larger than \(\kappa_f\), 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],

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

for every \( \epsilon > 0 \) and some \( \kappa_0, \kappa_\epsilon \), where \( \kappa_\epsilon \) depends only on \( f \) and \( \epsilon \). 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 obtain 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. \( \square \)

As is usual, we speak of the rank of a curve \( C \) when we mean the rank of its Jacobian. Thus \( \text{rank}(C) \) and \( \text{rank}(J_C) \) 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 \( 0 < \epsilon < 1/2 \), let

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

Then

\[
\#S \ll \epsilon \cdot 2^{(\alpha + O_\epsilon(x_0^{-2})) \cdot \text{rank}(C_d(K))},
\]

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

**Proof.** Let \( C = C_1 \). Let \( c_0 \) be as in Proposition 4.27 \( \phi_{d,c_0} \) 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 \( \text{rank}(J_{C_d}(K)) + 1 \). 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

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

with torsion kernel such that the inner product in \( \mathbb{R}^{\text{rank}(J_{C_d}(K)) + 1} \) 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 \( \iota \) 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],

\[
(1 - \epsilon)^2\kappa_0 x_0 - \kappa_\epsilon \leq |\phi_{d,c_0}(P)|^2 \leq (1 + \epsilon)^2\kappa_0 x_0 + \kappa_\epsilon
\]

for some \( \kappa_0, \kappa_\epsilon \), the latter depending on \( \epsilon \). For any \( P_1, P_2 \in C_d(\mathbb{Q}), P_1 \neq P_2 \), we have by Proposition 4.27 that

\[
\langle \phi_{d,c_0}(P_1), \phi_{d,c_0}(P_2) \rangle \leq \frac{|\phi_{d,c_0}(P_1)|^2 + |\phi_{d,c_0}(P_2)|^2}{4} + O(1).
\]
Hence, for \( P_1 = (x_1, y_1), P_2 = (x_2, y_2) \) in \( S \), \( P_1 \neq P_2 \),

\[
\frac{\langle t(\phi_{d,c_0}(P_1)), t(\phi_{d,c_0}(P_2)) \rangle}{|t(\phi_{d,c_0}(P_1))||t(\phi_{d,c_0}(P_2))|} = \frac{\langle \phi_{d,c_0}(P_1), \phi_{d,c_0}(P_2) \rangle}{|\phi_{d,c_0}(P_1)||\phi_{d,c_0}(P_2)|} \leq \frac{|\phi_{d,c_0}(P_1)| + |\phi_{d,c_0}(P_2)|}{4} + O(x_0^{-2})
\]

\[
\leq \frac{(1-\epsilon)^2 + (1+\epsilon)^2}{4} + O(x_0^{-2})
\]

\[
= \frac{(1 + 6\epsilon^2 + \epsilon^4)/(1 - \epsilon^2)^2}{2} + O(x_0^{-2}).
\]

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 \( 60^\circ - \epsilon \) between any two of them. As before, we can apply (4.18). We obtain

\[
\#\ell(S) \ll 2^{\alpha + O(x^2) + O(x_0^{-2})} + \text{an implied constant}
\]

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

\[
\{(x, y, z) \in \mathbb{Z}^3 : \| x \| \leq N^{1-\epsilon}, dy^2 = f(x, z) \}.
\]

Then

\[
\#S \ll 2^{\alpha + O((\log N)^{-2})} \text{rank}(C_d),
\]

where \( \alpha \) is as in (4.18) and the implied constants in \( \ll \) and \( O(x_0^{-2}) \) depend only on \( f \) and \( \epsilon \).

**Proof.** Immediate from Prop. 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

\[
\delta(N) = \{-N \leq x, z \leq N : \gcd(x, y) = 1, \exists p > N^{1/2} \text{ s.t. } p^2 | f(x, z) \}. \]

Then, for every \( \epsilon > 0 \),

\[
(4.24) \quad \delta(N) \ll X(\log X)^{-\beta + \epsilon},
\]

where \( \beta \) is given in Figure 2 in terms of the Galois group of the splitting field of \( f(x, 1) = 0 \). The implied constant depends only on \( f \) and \( \epsilon \).

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

\[
\delta(N) \leq \sum_{N^{1/2} < p < \sqrt{A/M}} \#\{-N \leq x, z \leq N : p^2 | f(x)\}
\]

\[
+ \{-N^{1-\epsilon} \leq x, z \leq N^{1-\epsilon} : \gcd(x, z) = 1, \exists p > N^{1/2} \text{ s.t. } p^2 | f(x, z)\}
\]

\[
+ \sum_{1 \leq |d| \leq M} \#\{x, z \in \mathbb{Z}^2 : N^{1-\epsilon} \leq \max(|x|, |z|) \leq N, dy^2 = f(x, z)\}.
\]
Let $M \leq N^2$. 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 $N^{2-\epsilon}$. It remains to bound
\[
\sum_{1 \leq |d| \leq M} B(d),
\]
where
\[
B(d) = \#\{x, z \in \mathbb{Z}^2 : N^{1-\epsilon} \leq \max(|x|, |z|) \leq N, dy^2 = f(x, z)\}.
\]

By Corollary 4.30,
\[
B(d) \ll 2^{(\alpha + O(\epsilon^2) + O((\log N)^{-2})) \text{rank}(C_d)}.
\]

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
\[
S(M) = \sum_{1 \leq d \leq M, d \text{ square-free}} 2^{(\alpha + O(\epsilon^2)) \text{rank}(C_d)}.
\]

Corollary 4.25 gives us $S(M) \ll M(\log M)^{\delta-1+O(\epsilon^2)}$, where $\delta$ is as in Figure 1. Set $M = N^2(\log N)^{-\frac{2}{3}}$. Then
\[
S(M) \ll N^2(\log N)^{\frac{1}{3}\delta-1+O(\epsilon^2)}, \quad \frac{N^3 M^{-1/2}}{\log N} \ll N^2(\log N)^{\frac{1}{3}\delta-1+O(\epsilon^2)}.
\]

\[\square\]

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 $x \leq N$ for which $f(x)$ is square-free is given by

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

where

$$\beta = \begin{cases} 0.8061 \ldots & \text{if the discriminant of } f \text{ is a square,} \\ 0.6829 \ldots & \text{if the discriminant of } f \text{ is not a square}, \end{cases}$$

$$\ell(m) = \#\{x \in \mathbb{Z}/m : f(x) \equiv 0 \mod m\}.$$

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

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

where $\epsilon$ is an arbitrarily small positive number, $\beta$ is given in Figure 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 $\epsilon$, $\deg_{\text{irr}}$ denotes the degree of the irreducible factor of $f$ of largest degree, and

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

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 Prop. 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 $\deg_{\text{irr}}(P(x)) = 2$ was dealt with by Estermann [Es], the case $\deg_{\text{irr}}(P(x)) = 3$ by Hooley ([Hoo], Ch. IV). All entries for $P(x, y)$ homogeneous, $3 \leq \deg_{\text{irr}}(P(x)) \leq 6$, are due to Greaves [Gre]. The bound given in the main theorem of [Gre] for $\deg_{\text{irr}} = 6$ 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 $\{1, 2, \ldots, N\}^{\deg K}$ 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 Prop. 3.2 and Cor. 3.3 will accommodate the required change in the objects of study.

7. 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 $\text{Disc} P$ for the discriminant of a polynomial $P \in \mathcal{O}_K[x]$. If $P$ is square-free, then $\text{Disc}(P)$ is a non-zero element of $\mathcal{O}_K$, and

$$\gcd(P(x), P'(x)) | \text{Disc}(P)$$

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

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

$$P(x) \equiv 0 \mod p^n$$

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

Proof. Let $\pi$ 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 $P = P_1 \cdot P_2 \cdots \cdot P_l$, $P_i \in \mathcal{O}_K$, $P_i$ irreducible.

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

$$v_p(P'(x)) = v_p(\sum_j P_j'(x) \cdot P_1(x) \cdots \cdot \hat{P_j}(x) \cdots \cdot P_n(x))$$

$$\geq \min_j (v_p(P(x)) - v_p(P_j(x))),$$

$$\min(v_p(P'(x)), v_p(P(x))) \leq v_p(\text{Disc} P),$$
we have that

\[ \min_j (v_p(P(x)) - v_p(P_j(x))) \leq v_p(\text{Disc } P) \]

and hence

\[ v_p(P_i(x)) \geq v_p(P_i(x)) - v_p(\text{Disc } P) \geq n - v_p(\text{Disc } P) \geq 2v_p(\text{Disc } P) + 1. \]

On the other hand \( \gcd(P_i(x), P'_i(x)) | \text{Disc } P \), and thus

\[ v_p(P'_i(x)) \leq v_p(\text{Disc } P). \]

By Hensel’s lemma we can conclude that \( P_i \) is linear. Since \( v_p(P_i(x)) \geq n - v_p(\text{Disc } P) \), \( x \) is a root of

\[ P_i(x) \equiv 0 \mod p^{n - v_p(\text{Disc } P)}. \]

Since \( P_i \) is linear and not divisible by \( p \), it has at most one root in the ring \( \mathcal{O}_K/p^n \). There are at most \( v_p(\text{Disc } P) \) elements of \( \mathcal{O}_K/p^n \) reducing to this root. Summing over all \( i \) we obtain that there are at most \( l \cdot v_p(\text{Disc } P) \) roots of \( P(x) \equiv 0 \mod p^n \) in \( \mathbb{Z}/p^n \). Since \( l \leq \deg P \), the statement follows.

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

**Lemma A.2.** Let \( K \) be a number field. Let \( m \) be a non-zero ideal of \( \mathcal{O}_K \). Let \( P \in \mathcal{O}_K[x] \) be a square-free polynomial. Then

\[ \{ x \in \mathbb{Z} : P(x) \equiv 0 \mod m \} \]

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

**Proof.** By Lemma A.1 for every \( p|m \), the equation

\[ P(x) \equiv 0 \mod p^n \]

has at most \( |\text{Disc } P| p^{-3} \deg P \) roots in \( \mathcal{O}_K/p^n \). For any ideal \( a \), the intersection of \( \mathbb{Z} \) with a set of the form

\[ \{ x \in \mathcal{O}_K : x \equiv x_0 \mod a \} \]

is either the empty set or an arithmetic progression of modulus \( h(a) \). This is in particular true for \( a = p^n \); the set

\[ \{ x \in \mathbb{Z} : x \equiv x_0 \mod p^n \} \]

is the union of at most \( |\text{Disc } P| p^{-3} \deg P \) arithmetic progressions of modulus \( h(p^n) \).

Now consider a rational prime \( p \) at least one of whose prime ideal divisors divides \( m \). Write \( m = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} m_0 \), where \( p_1, \ldots, p_k | p \), \( \gcd(m_0, p) = 1 \), \( \frac{m_1}{e_1} \geq \frac{m_2}{e_2} \geq \cdots \geq \frac{m_k}{e_k} \) and \( e_1, \ldots, e_k \) are the ramification degrees of \( p_1, \ldots, p_k \).

The set

\[ \{ x \in \mathbb{Z} : x \equiv x_0 \mod p_1^{n_1} \cdots p_k^{n_k} \} \]

is the intersection of the sets

\[ \{ x \in \mathbb{Z} : x \equiv x_0 \mod p_j^{n_j} \}, \quad 1 \leq j \leq k. \]
At the same time, it is a disjoint union of arithmetic progressions of modulus
\[ h(p_1^{n_1} \cdots p_k^{n_k}) = h(p_1^{n_1}). \]
Since
\[ \{x \in \mathbb{Z} : x \equiv x_0 \mod p_1^{n_1}\} \]
is the disjoint union of at most \( |\text{Disc } P|^{-3} \deg P \) arithmetic progressions of modulus \( h(p_1^{n_1}) \), it follows that
\[ \{x \in \mathbb{Z} : x \equiv x_0 \mod p_1^{n_1} \cdots p_k^{n_k}\} \]
is the disjoint union of at most \( |\text{Disc } P|^{-3} \deg P \) arithmetic progressions of modulus \( h(p_1^{n_1}) = h(p_1^{n_1} \cdots p_k^{n_k}). \) 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
\[ S = \{(x, y) \in \mathbb{Z}^2 : \gcd(x, y) = 1, \mathfrak{m}|P(x, y)\} \]
is the union of at most \( |\text{Disc } P|^{-3} \tau_2 \deg P(\text{rad}(h(\mathfrak{m}))) \) 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 \( \mathfrak{p}|\mathfrak{m} \). Let \( n = \nu_\mathfrak{p}(\mathfrak{m}) \). Let \( r_1, r_2, \ldots, r_k \in \mathcal{O}_K/\mathfrak{p}^n \) be the roots of \( P(r, 1) \equiv 0 \mod \mathfrak{p}^n \). Let \( r_1', r_2', \ldots, r_k' \in \mathcal{O}_K/\mathfrak{p}^n \) be such roots of \( P(1, r) \equiv 0 \mod \mathfrak{p}^n \) as satisfy \( \mathfrak{p}|r \). Then the set of solutions to \( P(x, y) \equiv 0 \mod \mathfrak{p}^n \) in
\[ \{(x, y) \in \mathbb{Z}^2 : \mathfrak{p} \nmid \gcd(x, y)\} \]
is the union of the disjoint sets
\[ \{(x, y) \in \mathbb{Z}^2 : \mathfrak{p} \nmid \gcd(x, y), x \equiv r, y \mod \mathfrak{p}^n\}, \]
\[ \{(x, y) \in \mathbb{Z}^2 : \mathfrak{p} \nmid \gcd(x, y), y \equiv r, x \mod \mathfrak{p}^n\}. \]
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
\[ \frac{\text{Area}(S \cap [-N, N]^2)}{[\mathbb{Z}^2 : L]} \prod_p \left( 1 - \frac{1}{p^2} \right) + O(N \log N). \]
The implied constant is absolute.

**Proof.** We can write \( \#(\{1 \leq x, y \leq N : \gcd(x, y) = 1\} \cap S \cap L) \) as
\[ \sum_{m=1}^{N} \mu(m) \cdot \#(\{1 \leq x, y \leq N : m|x, m|y \cap S \cap L\}). \]
Since \( L \) is not of the form \( \ell L', \ell > 1, L' \subset \mathbb{Z}^2 \) a lattice, we have that \( \frac{1}{m}(L \cap m\mathbb{Z}^2) \) is a lattice of index \([\mathbb{Z}^2 : \frac{1}{m}(L \cap m\mathbb{Z}^2)] = [\mathbb{Z}^2 : L] \). Thus
\[ \#(\{1 \leq x, y \leq N : m|x, m|y \} \cap S \cap L) = A \cdot N^2/m^2[\mathbb{Z}^2 : L] + O(N/m), \]
where $A = \text{Area}(S \cap [-1, 1]^2)$. Hence

$$
\#(\{1 \leq x, y, \leq N : \gcd(x, y) = 1\} \cap S \cap L) \\
= A \cdot \sum_{m=1}^{N} \mu(m)N^2/m^2 [\mathbb{Z}^2 : L] + O(N \log N),
$$

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

□

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

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

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

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

If $M_0 \geq \frac{[\mathbb{Z}^2 : L]}{2N}$ we are done. Assume $M_0 < \frac{[\mathbb{Z}^2 : L]}{2N}$. Suppose

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

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 $\#(\{-N \leq x, y \leq N : \gcd(x, y) = 1\} \cap L)$ 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 $\sqrt{x_0^2 + y_0^2} \cdot \sqrt{x_1^2 + y_1^2} \leq \sqrt{2} M_0 \cdot \sqrt{2} N = 2 M_0 N$. Since we have assumed $M_0 < \frac{[\mathbb{Z}^2 : L]}{2N}$ we arrive at a contradiction. □

**APPENDIX B. Divisor sums**

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

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

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

where the implied constant depends only on $\epsilon$. 
Proof. For every positive \( k \),
\[
\sum_{p > k} \frac{1}{p \log p} \leq \frac{1}{\log k} \left( \sum_{k \leq p < k^2} \frac{1}{p} + \frac{1}{2} \sum_{k^2 \leq p < k^4} \frac{1}{p} + \frac{1}{4} \sum_{k^4 \leq p < k^8} \frac{1}{p} + \ldots \right)
\]
\[
= \frac{\log \log k^2 - \log \log k + O(1/(\log k))}{\log k}
+ \frac{\log \log k^4 - \log \log k^2 + O(1/(\log k))}{2 \log k} + \ldots
\]
\[
= \frac{2(\log 2 + O(1/(\log k)))}{\log k}.
\]
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
\[
\sum_{n \text{ square-free}} \prod_{p \mid n} \frac{\log X}{p \log p} = \prod_{p \leq k} \left( 1 + \frac{\log X}{p \log p} \right) \prod_{p > k} \left( 1 + \frac{\log X}{p \log p} \right)
\]
\[
\ll \prod_{p \leq k} \log X \prod_{p > k} \left( 1 + \frac{1}{p \log p} \right) \log X
\]
for \( N > 2 \). Therefore
\[
\sum_{1 \leq n \leq N} \prod_{p \mid n} \frac{\log n}{p \log p} \ll e^{2 \log 2 \log X / \log k + O(1/(\log X/(\log k)^2))} \prod_{p \leq k} \log X
\]
\[
\ll e^{2 \frac{\log 2 \log X}{\log k} + O(\frac{\log X}{(\log k)^2})} e^{\frac{\log \log k}{\log k} + O\left(\frac{\log \log X}{(\log k)^2}\right)}
\]
Set \( k = \log X / \log \log X \). We obtain
\[
\sum_{1 \leq n \leq N} \prod_{p \mid n} \frac{\log X}{p \log p} \ll e^{(2 + \epsilon') \log X / \log \log X}
\]
for every \( \epsilon' > 0 \), where the implied constant depends only on \( \epsilon' \). \( \square \)

**Lemma B.2.** Let \( c > 0 \) be given. For every \( \epsilon > 0 \),
\[
\frac{1}{N} \sum_{1 \leq n \leq N \atop n \text{ square-free}} \tau(n) \prod_{p \mid n} \frac{c \log N}{p \log p} \ll N^\epsilon,
\]
where the implied constant depends only on \( c_0 \) and \( \epsilon \).

**Proof.** Clearly
\[
\frac{1}{N} \sum_{1 \leq n \leq N \atop n \text{ square-free}} \tau(n) \prod_{p \mid n} \frac{c \log N}{p \log p} \leq \frac{1}{N} \sum_{1 \leq n \leq N \atop n \text{ square-free}} \prod_{p \mid n} \frac{2c \log N}{p \log p} \ll \sum_{n=1}^{\infty} \prod_{p \mid n} \frac{\log N^{2c}}{p \log p}.
\]
Proceed as in Lemma B.1. \( \square \)
References

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

[Ca] Cassels, J. W. S., The Mordell-Weil group of curves of genus 2, Arithmetic and geometry, Vol. I, 27–60, Prog. Math. 35, Birkhäuser, Boston, Mass., 1983.

[CF] Cassels, J. W. S., and E. V. Flynn, Prolegomena to a middletrow arithmetic of curves of genus 2, London Math. Soc. Lecture Note Ser. 230, Cambridge University Press, Cambridge, 1996.

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

[CS] Conway, J. H., and N. J. A. Sloane, Sphere packings, lattices and groups, Grundlehren der Mathematischen Wissenschaften, 290, Springer-Verlag, New York, 1988.

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

[FPS] Flynn, E. V., Poonen, B., and E. Schaefer, Cycles of quadratic polynomials and rational points on a genus-2 curve, Duke Math. J. 90 (1997), no. 3, 435–463.

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

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

[GS] Gross, R., and J. Silverman, S-integer points on elliptic curves, Pacific J. Math. 167 (1995), no. 2, 263–288.

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

[He2] Helfgott, H. A., Root numbers and the parity problem, Ph.D. thesis, Princeton University, http://www.arxiv.org/abs/math.NT/0305435

[Hoo] Hookey, C., Applications of sieve methods to the theory of numbers, Cambridge University Press, Cambridge, 1976.

[La] Lang, S., Fundamentals of diophantine geometry, Springer–Verlag, New York, 1983.

[KL] Kabtjanski˘ı, G. A., and V. I. Levenˇ ste˘ ın, Bounds for packings on the sphere and in space, Problemy Peredači Informacii 14 (1978), no. 1, 3–25.

[Maz] Mazur, B., Rational points on modular curves, Modular functions of one variable, V, Lecture Notes in Mathematics, 601, Springer, Berlin, 1977.

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

[PT] Parson, A., and J. Tull, Asymptotic behavior of multiplicative functions, J. Number Theory 10 (1978), no. 4, 395–420.

[Ra] Ramsay, K., personal communication.

H. A. HELFGOTT, DÉPARTEMENT DE MATHEMATIQUES ET STATISTIQUE, UNIVERSITÉ DE MONTRÉAL, MONTRÉAL, QC H3C 3J7, CANADA
E-mail address: helfgott@dms.umontreal.ca