ON REPRESENTATION OF INTEGERS BY BINARY QUADRATIC FORMS

J. Bourgain, E. Fuchs

Abstract. Given a negative $D > -(\log X)^{\log 2-\delta}$, we give a new upper bound on the number of square free integers $< X$ which are represented by some but not all forms of the genus of a primitive positive definite binary quadratic form f of discriminant D. We also give an analogous upper bound for square free integers of the form $q + a < X$ where q is prime and $a \in \mathbb{Z}$ is fixed. Combined with the 1/2-dimensional sieve of Iwaniec, this yields a lower bound on the number of such integers $q + a < X$ represented by a binary quadratic form of discriminant D, where D is allowed to grow with X as above. An immediate consequence of this, coming from recent work of the authors in [BF], is a lower bound on the number of primes which come up as curvatures in a given primitive integer Apollonian circle packing.

§0. Introduction

Let $f(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$ be a primitive positive-definite binary quadratic form of negative discriminant $D = b^2 - 4ac$. For $X \to \infty$, we denote by $U_f(X)$ the number of positive integers at most X that are representable by f. The problem of understanding the behavior of $U_f(X)$ when D is not fixed, i.e. $|D|$ may grow with X, has been addressed in several recent papers, in particular in [Bl] and [B-G]. What is shown in these papers, on a crude level, is that there are basically three ranges of the discriminant for which one should consider $U_f(X)$ separately $\big($we restrict ourselves to discriminants satisfying $\log|D| \leq \mathrm{O}(\log\log X)\big)$

(i) $|D| \ll (\log X)^{(\log 2)-\varepsilon}$. Then $U_f(X) \gg_\varepsilon X(\log X)^{-\frac{1}{2}-\varepsilon}$ (0.1)

(ii) $|D| \gg (\log X)^{2(\log 2)+\varepsilon}$. Then $U_f(X) \asymp \frac{X}{\sqrt{D}}$ (0.2)

(iii) The intermediate range.

As Blomer and Granville explain in [B-G], this transitional behavior is due to the interplay between the size h of the class group $\mathcal{C}$ and the typical number of prime factors of an integer $n \sim X$. A precise elaboration of the underlying heuristics was kindly communicated by V. Blomer to the authors and is reproduced next. The number of integers $n < X$ with k prime factors p split in the quadratic number field (i.e. $(\frac{D}{p}) = 1$) is of the order

$$\frac{X}{\log X}\ \frac{1}{2^k}\ \frac{(\log\log X)^{k-1}}{(k-1)!}. \tag{0.3}$$

Note that summation of (0.3) over k gives $\frac{X}{\sqrt{\log X}}$, which is the number of integers at most X represented by some form of discriminant D.

The first author was partially supported by NSF Grants DMS-0808042 and DMS-0835373

The second author was supported by NSF Grant DMS-0635607

Moreover, applying Stirling's formula, we see that the main contribution comes from integers with $k \sim \frac{1}{2} \log\log X$ prime factors.

Next, ignoring ambiguous classes, these k primes yield 2^k classes (with possible repetition) in $\mathcal{C}$ that represent the given integer n. Hence, roughly speaking, one would expect that typically n is represented by each class of its genus provided $2^k \gg h$, which amounts to

$$h < (\log X)^{\frac{\log 2}{2} - \varepsilon} \tag{0.4}$$

corresponding to alternative (i).

On the other hand, if D is sufficiently large, the 2^k classes will be typically distinct. Assuming some mild form of equidistribution in the class group when varying n, we expect for the number of integers $n < X$ with k prime factors represented by a given class to be of order

$$\frac{2^k}{h} \cdot (0.3) = \frac{X}{h \log X} \, \frac{(\log\log X)^{k-1}}{(k-1)!} \tag{0.5}$$

with total contribution $\mathrm{O}\Big(\frac{X}{h}\Big)$, attained when $k \sim \log\log X$ (at this level of the discussion, there is no difference between h and $\sqrt{D}$).

In this paper, we consider only the lower range (i). Our aim is to substantiate further the heuristic discussed above according to which, typically, all classes of the genus of $n \sim X$, n representable by a form of discriminant D, do actually represent n.

More precisely, we prove the following (as consequence of Theorem 2 in [B-G]).

Theorem 2'. *Let D be a negative discriminant satisfying*

$$|D| < (\log X)^{\log 2 - \delta} \tag{0.6}$$

for some fixed $\delta > 0$. Then there is $\delta' = \delta'(\delta) > 0$ such that

$\#\{n \sim X$; n square free, representable by some form of discriminant D but not by all forms of the genus$\}$

$$< \frac{X}{(\log X)^{\frac{1}{2} + \delta'}}. \tag{0.7}$$

Note that though [Bl], [B-G] establish (0.1) (in fact in a more precise form, cf. Theorem 5 in [B-G]), their results do not directly pertain to the phenomenon expressed in Theorem 2'. As pointed out in [B-G], it was shown on the other hand by Bernays that almost all integers represented by some form in a given genus can be represented by all forms in the genus, but assuming the much stronger restriction

$$D \ll (\log\log X)^{\frac{1}{2} - \varepsilon}. \tag{0.8}$$

A result in the same spirit was also obtained by Golubeva [Go].

The proof of Theorem 2' rests on a general result from arithmetic combinatorics (Theorem 1 below) that we describe next. Assume G a finite abelian group ($G = \mathcal{C}^2$ in our application) in which group operation will be denoted additively. Given a subset $A \subset G$, we introduce the set

$$s(A) = \Big\{ \sum x_i; \{x_i\} \text{ are distinct elements of } A \Big\}. \tag{0.9}$$

The issue is then to understand what it means for A that $s(A) \neq G$, which is the undesirable outcome for our purposes. It turns out that there are basically two possibilities. In the first, A is contained, up to a bounded number of elements, in a proper subgroup H of G of bounded index [G:H]. In our application to the class group in Section 2, we give an upper bound on the number of possibilities for such A.

The second scenario is as follows. There are k elements $x_1, \dots, x_k \in A$ with

$$k < (1+\varepsilon)\frac{\log |G|}{\log 2} \tag{0.10}$$

and a subset $\Omega_{x_1,\dots,x_k} \subset G$ (determined by $x_1, \dots, x_k$), such that $A \subset \Omega_{x_1,\dots,x_k}$ and

$$|\Omega_{x_1,\dots,x_k}| < \varepsilon |G| \tag{0.11}$$

(we are assuming here that $|G|$ is large). Note that this second scenario occurs in some sense very rarely. Specifically, denote by K the upper bound on k in (0.10), and let $|A| \sim m$, where in our application $m \sim K \cdot (1+a)$ for a small fixed $a > 0$, and m corresponds to the typical number of prime factors of an integer $< X$ represented by the genus of f. There are $\binom{h'}{m}$ possible choices for such A, and of these at most $\binom{h'}{K} \cdot \binom{\varepsilon h'}{m-K}$ sets A which fall into the second scenario. For small ε, the latter is much smaller than $\binom{h'}{m}$, and in this sense this undesirable scenario is relatively rare.

To prove Theorem 1, one applies the greedy algorithm. Thus given $x_1, \dots, x_k \in A$, we select $x_{k+1} \in A$ as to optimize the size of $s(x_1, \dots, x_{k+1})$. If we do not reach $s(x_1, \dots, x_k) = G$ with k satisfying (0.10), then

$$A \subset \{x_1, \dots, x_k\} \cup \Omega \tag{0.12}$$

where the elements $x \in \Omega$ have the property that

$$|s(x_1, \dots, x_k, x)| \approx |s(x_1, \dots, x_k)|. \tag{0.13}$$

Assuming Ω fails (0.11), the first alternative is shown to occur. The argument involves combinatorial results, such as a version of the Balog-Szemeredi-Gowers theorem and also Kneser's theorem. The reader is referred to the book [T-V] for background material on the matter.

Once Theorem 1 is established, deriving Theorem 2 is essentially routine. We make use, of course, of Landau's result [L2] (established in [Bl] with uniformity in the discriminant), on the distribution of the primes represented by a given class $C \in \mathcal{C}$ – namely, for $\mathcal{P}_C$ the set of primes represented by a class C,

$$|\{p \in \mathcal{P}_C; p \leq \xi\}| = \frac{1}{\varepsilon(C)h}\int_1^\xi \frac{dt}{\log t} + C(\xi e^{-c\sqrt{\log \xi}}) \tag{0.14}$$

for $\xi \to \infty$, with $\varepsilon(C) = 2$ if C is ambiguous and $\varepsilon(C) = 1$ otherwise.

The nontrivial upper bound (0.7) is then obtained by excluding certain additional prime divisors, i.e. satisfying $\left(\frac{D}{p}\right) \neq -1$, using standard upper bound sieving.

The same approach permits to obtain a similar result considering now shifted primes, i.e. integers n of the form $n = a + q$ with a fixed and q a prime number. Thus

Theorem 3'. *Under the assumption (0.6), fixing $a \in \mathbb{Z}$, we have*
$|\{q + a \sim X$; *q prime, $q + a$ squarefree representable by some form of discriminant D but not by all forms of the genus*$\}$ $|$

$$< \frac{X}{(\log X)^{\frac{3}{2}+\delta'}}. \tag{0.15}$$

On the technical side, only crude sieving bounds are needed for our purpose and they can be obtained by the simple inclusion/exclusion principle without the need of Brun's theory. The arguments covering the specific problem at hand were included in the paper (see Lemmas 4 and 5), which turned out to be more convenient than searching for a reference. Note that the proof of Lemma 5 involves sieving in the ideals and the required remainder estimates are provided by Landau's extension of the Polya-Vinogradov inequality for Hecke characters [L1].

The motivation behind Theorem 3' lies in a result due to H. Iwaniec [Iw] on the number of shifted primes that are representable by the genus of a quadratic form. This in turn is applicable to counting primes which appear as curvatures in a primitive integer Apollonian circle packing using a method similar to that in [BF], where the authors prove that the integers appearing as curvatures in a primitive integer Apollonian packing make up a positive fraction of $\mathbb{Z}$.

Specifically, let P be a primitive integer Apollonian packing, and let $a \neq 0$ denote a curvature of a circle in P. From [BF], we have that the set S_a of integers less than X represented by certain shifted binary quadratic forms $f_a(x, y) - a$, where the discriminant $D(f_a) = -4a^2$, is contained in the set of curvatures of circles in P. Let $\mathfrak{P}_a \subset S_a$ denote the set of primes in S_a. We may then compute a lower bound for the number of primes less than X appearing as curvatures in P by bounding

$$|\bigcup_a \mathfrak{P}_a|$$

where the a's range over a set of our choice. The aim is to use the $\frac{1}{2}$-dimensional sieve of Iwaniec to first determine the cardinality of $\mathfrak{P}_a$. In [Iw], Iwaniec proves upper and lower bounds for the number of primes less than N represented by $\phi(x, y) + A$, where $\phi(x, y)$ is a positive definite binary quadratic form and A is an integer. He shows

$$\frac{X}{(\log X)^{3/2}} \ll S(X, \phi, a) \ll \frac{X}{(\log X)^{3/2}}$$

where $S(X, \phi, a)$ denotes the number of primes less than X represented by $\phi(x, y) + A$. Here the discriminant of ϕ is fixed, and the bounds above are obtained by considering the count over all forms in the genus of ϕ: namely, for fixed discriminant, bounds for $S(X, \phi, a)$ are easily derived from bounds for

$$S_1(X, \phi, a) = \sum_{\substack{p \leq X \\ (x,y)=1, f \in R_\phi \\ p = f(x,y)+a}} 1$$

where R_ϕ denotes the genus of ϕ. In order to apply this to finding bounds for $|\mathfrak{P}_a|$ where a is allowed to grow with X, we must understand both how $S_1(X, \phi, a)$ depends on the discriminant of ϕ, and how S relates to S_1 in the case that D is not fixed. The latter is explained by Theorem 3' for D satisfying (0.6), while the former is done via a careful analysis of the dependence on the discriminant in [Iw] for $D < \log X$. This is discussed in the Appendix. Note that in the application to Apollonian packings, the discriminant of ϕ is always of the form $-4a^2$, but our results apply to a more general discriminant.

Indeed, Theorem 1 in [Iw] combined with Theorem 3' above implies the following

Corollary 4. *Let $D < 0$ satisfy (0.6) and f be a primitive positive definite binary form of discriminant D. Then*

$$|\{q + a \sim X; q \text{ prime, } q + a \text{ representable by } f\}| \gg \frac{X}{(\log X)^{\frac{3}{2}+\varepsilon}} \tag{0.16}$$

(we assume here $a \in \mathbb{Z}$ fixed for simplicity).

Acknowledgement: The authors are grateful to V. Blomer for several private communications, as well as B. Green for helpful suggestions on a previous version of this paper.

§1. A result in combinatorial group theory

The aim of this section is to prove Theorem 1 below.

(1). Let G be an abelian group, $|G| = h'$.

For $A \subset G$, denote by

$$s(A) = \Big\{ \sum x_i;\ \{x_i\} \text{ distinct elements of } A \Big\} \tag{1.0}$$

the set of sums of distinct elements of A.

Assume $s(A) \neq G$. We would like to specify the structure of such A.

Start with the following algorithm. Take $x_1 \in A$. Assume we have obtained $x_1, \dots, x_j$, take x_{j+1} as to maximize

$$s(x_1, \dots, x_{j+1}).$$

Let $\delta_j = \frac{|s(x_1,\dots,x_j)|}{h'}$. One has

$$\begin{aligned} |s(x_1, \dots, x_j, x)| &= |s(x_1, \dots, x_j) \cup \big(s(x_1, \dots, x_j) + x\big)| \\ &= 2\big|s(x_1, \dots, x_j)\big| - \big|s(x_1, \dots, x_j) \cap \big(s(x_1, \dots, x_j) + x\big)\big|. \end{aligned}$$

Hence

$$\mathbb{E}_x[|s(x_1, \dots, x_j, x)|] = 2\delta_j h' - \delta_j^2 h' = \delta_j(2 - \delta_j)h'. \tag{1.1}$$

On the other hand, for all x

$$|s(x_1, \dots, x_j, x)| \leq (2\delta_j)h'. \tag{1.2}$$

Fix $\varepsilon > 0$. For $\delta_j < \frac{1}{2}$, define

$$\Omega = \{x \in G; |s(x_1, \dots, x_j, x)| < (2 - \varepsilon)\delta_j h'\}.$$

Then, from (1.1), (1.2)

$$\mathbb{E}_x[|s(x_1, \dots, x_j, x)|] \leq (2\delta_j h')\Big(1 - \frac{|\Omega|}{h'}\Big) + (2 - \varepsilon)\delta_j h' \frac{|\Omega|}{h'}$$

implying

$$|\Omega| < \frac{\delta_j}{\varepsilon} h'. \tag{1.3}$$

For $\delta_j > \frac{1}{2}$, define

$$\Omega = \{x \in G; |s(x_1, \dots, x_j, x)| < \big(1 - (1-\delta_j)^{3/2}\big)h'\}.$$

Similarly

$$|\Omega| < (1-\delta_j)^{1/2} h'. \tag{1.4}$$

It follows from (1.3) that either

(1.5) there exist $x_1, \dots, x_k \in A$ s.t.

$$|s(x_1, \dots, x_k)| > \varepsilon^2 h' \tag{1.6}$$

with

$$k < \frac{\log h'}{\log 2 - \frac{\varepsilon}{2}} \tag{1.7}$$

or

(1.8) There exist elements $x_1, \dots, x_k \in A$ and a set $\Omega_{x_1,\dots,x_k} \subset G$ satisfying

$$A \subset \{x_1, \dots, x_k\} \cup \Omega_{x_1,\dots,x_k} \tag{1.9}$$

$$k < \frac{\log h'}{\log 2 - \frac{\varepsilon}{2}} \tag{1.10}$$

$$|\Omega_{x_1,\dots,x_k}| < \varepsilon h'. \tag{1.11}$$

(2). Let $A_1 \subset A$ s.t.

$$\delta h' = s(A_1) > \varepsilon^2 h'. \tag{2.1}$$

Fix $\varepsilon_1 > 0$ and define

$$\Omega = \{x \in G; |s(A_1 \cup \{x\})| < (1-\varepsilon_1)|s(A_1)| + \varepsilon_1 h'\}. \tag{2.2}$$

If $(A \backslash A_1) \cap \Omega^c \neq \emptyset$, we add an element and increase the density from δ in (2.1) to $(1-\varepsilon_1)\delta + \varepsilon_1$.

Assume this process can be iterated r times.

We obtain a set A_1' such that $s(A_1')$ has density at least δ' satisfying

$$1 - \delta' = (1-\varepsilon_1)^r (1-\delta)$$

and thus $|s(A_1')| > (1-\varepsilon^2)h'$ for

$$r \sim \frac{\log \frac{1}{\varepsilon}}{\varepsilon_1}. \tag{2.3}$$

Continuing the process with A_1' and $\delta > 1 - \varepsilon^2 > \frac{1}{2}$ gives a subset $A_1'' \subset A$ so that $s(A_1'') = G$ and

$$|A_1''| \leq \frac{\log h'}{(\log 2) - \varepsilon} + c\frac{\log \frac{1}{\varepsilon}}{\varepsilon_1} + \log\log h' \tag{2.4}$$

unless we are in alternative (1.8) with (1.10) replaced by (2.4).

Thus it remains to analyze the case when the iteration fails.

If $|\Omega| < \varepsilon h'$, we are again in the situation (1.8) with (1.10) replaced by

$$\frac{\log h'}{\log 2 - \varepsilon} + c\frac{\log \frac{1}{\varepsilon}}{\varepsilon_1}.$$

Assume next Ω defined in (2.2) satisfies

$$|\Omega| > \varepsilon h'. \tag{2.5}$$

Denoting $B = s(A_1')$, we have by (2.1) and definition of Ω that

$$|B| > \varepsilon^2 h' \tag{2.6}$$

and

$$|B \cap (B + x)| > (1 - \varepsilon_1 \varepsilon^{-2})|B| \text{ for } x \in \Omega. \tag{2.7}$$

Hence

$$1_B * 1_{-B} > (1 - \varepsilon_1 \varepsilon^{-2})|B| \text{ on } \Omega \tag{2.8}$$

implying in particular that

$$|B| > (1 - \varepsilon_1 \varepsilon^{-2})|\Omega|. \tag{2.9}$$

(3). Assume (2.6)-(2.9).

Thus

$$\langle 1_B, 1_B * 1_\Omega \rangle = \langle 1_B * 1_{-B}, 1_\Omega \rangle \geq (1 - \varepsilon_1 \varepsilon^{-2})|B|\,|\Omega| \tag{3.1}$$

and

$$\|1_B * 1_\Omega\|_2 \geq (1 - \varepsilon_1 \varepsilon^{-2})|B|^{\frac{1}{2}}|\Omega|.$$

Squaring and using the fact that Ω is symmetric

$$\|1_B * 1_\Omega * 1_\Omega\|_2 \geq (1 - \varepsilon_1 \varepsilon^{-2})^2|B|^{\frac{1}{2}}|\Omega|^2$$

and for any given r (= power of 2)

$$\|1_B * 1_\Omega^{(r)}\|_2 \geq (1 - \varepsilon_1 \varepsilon^{-2})^r|B|^{\frac{1}{2}}|\Omega|^r. \tag{3.2}$$

(where $1_\Omega^{(r)}$ denotes the r fold convolution).

We will rely on the following lemma, which is originally due to Fournier [F].

Lemma 1. *Let μ be a probability measure on a discrete additive group G and assume (for small κ)*

$$\|\mu * \mu\|_2 > (1 - \kappa)\|\mu\|_2. \tag{3.3}$$

Then there is a subgroup H of G s.t.

$$\frac{1}{2}\|\mu\|_2^{-2} < |H| < 2\|\mu\|_2^{-2} \tag{3.3'}$$

and for some $z \in G$

$$\left\|\mu - \frac{1_{H-z}}{|H|}\right\|_1 < c\kappa^{1/12}. \tag{3.3"}$$

Proof.

From (3.3) we have

$$\sum_x \Big| \sum_y \mu(x-y)\mu(y)\Big|^2 > (1-\kappa)^2 \|\mu\|_2^2$$

and

$$\sum_{y_1, y_2} \langle \mu_{y_1}, \mu_{y_2}\rangle \mu(y_1)\mu(y_2) > (1-\kappa)^2\|\mu\|_2^2$$

implying

$$\begin{aligned} \sum \|\mu_{y_1} - \mu_{y_2}\|_2^2 \ \mu(y_1)\mu(y_2) &< 2\big(1-(1-\kappa)^2\big)\|\mu\|_2^2 \\ &< 4\kappa\|\mu\|_2^2. \end{aligned}$$

Hence there is $y_0 \in G$ such that

$$\sum \|\mu_y - \mu_{y_0}\|_2^2 \ \mu(y) < 4\kappa\|\mu\|_2^2$$

and by translation of μ, we may assume $y_0 = 0$, thus

$$\sum \|\mu_y - \mu\|_2^2 \ \mu(y) < 4\kappa\|\mu\|_2^2.$$

Denote

$$U = \{y \in G; \|\mu - \mu_y\|_2 < \kappa^{1/3}\|\mu\|_2\}.$$

Hence, from the preceding

$$\mu(G\backslash U) < 4\kappa^{1/3}.$$

Since

$$\frac{1}{|U|}\sum_{y\in U} \|\mu - \mu_y\|_2 < 4\kappa^{1/3}\|\mu\|_2$$

it follows by convexity that

$$\Big\|\mu - \mu * \frac{1_U}{|U|}\Big\|_2 < 4\kappa^{1/3}\|\mu\|_2$$

and in particular

$$\|\mu\|_2 \leq \frac{1}{|U|^{1/2}} + 4\kappa^{1/3}\|\mu\|_2$$

$$\|\mu\|_2 < \frac{1+4\kappa^{1/3}}{|U|^{1/2}}.$$

Next, write

$$\begin{aligned} \Big\|\mu - \frac{1_U}{|U|}\Big\|_2^2 &= \|\mu\|_2^2 + \frac{1}{|U|} - 2\frac{\mu(U)}{|U|} \\ &\leq \frac{2+10\kappa^{1/3} - 2(1-4\kappa^{1/3})}{|U|} \\ &< \frac{18\kappa^{1/3}}{|U|}. \end{aligned}$$

Hence

$$\Big\|\mu - \frac{1_U}{|U|}\Big\|_2 < \frac{5\kappa^{1/6}}{|U|^{1/2}} \tag{3.4}$$

and also

$$\begin{aligned}\Big\|\mu - \frac{1_U}{|U|}\Big\|_1 &\leq \mu(U^c) + \sum_{x\in U}\Big|\mu(x) - \frac{1}{|U|}\Big| \\ &\leq 4\kappa^{1/3} + |U|^{1/2}\Big\|\mu - \frac{1_U}{|U|}\Big\|_2 \\ &< 6\kappa^{1/6}. \end{aligned} \tag{3.5}$$

From (3.3), (3.4), (3.5), we have

$$\Big\|\frac{1_U}{|U|} * \frac{1_U}{|U|}\Big\|_2 > (1 - 20\kappa^{1/6})\frac{1}{|U|^{1/2}}$$

hence

$$E_+(U, U) = \|1_U * 1_U\|_2^2 > (1 - 40\kappa^{1/6}).|U|^3$$

where E_+ refers to the additive energy.[1]

We apply now some results from arithmetic combinatorics.

First, by (2.5.4), p.82 from [TV] (B-S-G in near-extreme case), there are subsets $U', U'' \subset U$ s.t.

$$|U'|, |U''| > (1 - 10\kappa^{1/12})|U|$$

and

$$|U' - U''| < (1 + 20\kappa^{1/12})|U|.$$

Thus from Ruzsa's triangle inequality, also

$$\begin{aligned}|U' - U'| \leq \frac{|U' - U''|^2}{|U''|} &< (1 + 60\kappa^{1/12})|U| \\ &< (1 + 80\kappa^{1/12})|U|. \end{aligned} \tag{3.6}$$

Next, we apply Kneser's theorem (see [TV], Theorem 5.5, p. 200).

For $T \subset G$, denote

$$\mathrm{Sym}_1(T) = \{x \in G; T + x = T\}$$

the symmetry group of T.

Then by Kneser's theorem, see [T-V]

$$|T - T| \geq 2|T| - |\mathrm{Sym}_1(T - T)|$$

and application with $T = U'$ gives

$$|\mathrm{Sym}_1(U' - U')| > (1 - 80\kappa^{1/12})|U'|. \tag{3.7}$$

[1] It has been pointed out to us by Ben Green that, in fact, from this bound on E_+ the desired result in (3.33") of Lemma 1 follows from Fournier's paper [F], as described in Theorems 1.3.3 and 1.4.6 of notes of Green- Wigderson [GW]. We include a different argument based on Kneser's theorem here.

Denoting $H = \operatorname{Sym}_1(U' - U'), H \subset U' - U$ and thus

$$\begin{aligned}|H|\,|U'| &\leq \sum_{z\in U'-U'-U'} |H \cap (U'+z)|\\ &\leq |U'-U'-U'|\,\max_z |H\cap(U'+z)|\\ &< (1+300\kappa^{1/12})|U'|\max_z |H\cap (U'+z)|\end{aligned}$$

from (3.6) and sumset inequalities. Therefore, there is some $z \in G$ s.t.

$$|(H-z)\cap U'| > (1+300\kappa^{1/12})^{-1}|H|$$

and in view of (3.7)

$$|U' \vartriangle (H-z)| < 1000\kappa^{\frac{1}{12}}|U|$$

and

$$|U \vartriangle (H-z)| < 1000\kappa^{\frac{1}{12}}|U|. \tag{3.8}$$

From (3.5), (3.8) we have

$$\Big\|\mu - \frac{1_{H-z}}{|H|}\Big\|_1 < C\kappa^{\frac{1}{12}}. \tag{3.9}$$

From (3.4), (3.8), we obtain (3.31) proving Lemma 1.

Returning to (2.5), (3.2), we have that

$$\Big\|\Big(\frac{1_\Omega}{|\Omega|}\Big)^{(r)}\Big\|_2$$

decreases in r and is between $\frac{1}{\sqrt{h'}}$ and $\frac{1}{\sqrt{\varepsilon h'}}$. Hence there is some τ

$$\log r < \frac{c}{\kappa}\log\frac{1}{\varepsilon} \tag{3.10}$$

such that $\mu = (\frac{1_\Omega}{|\Omega|})^{(r)}$ satisfies (3.3).

From (3.2), $(3.3')$, we conclude that

$$\begin{aligned}\Big\|1_B * \frac{1_H}{|H|}\Big\|_2 &\geq \big((1-\varepsilon_1\varepsilon^{-2})^r - c\kappa^{1/12}\big)|B|^{1/2}\\ &> (1-c\kappa^{1/12})|B|^{1/2}\end{aligned} \tag{3.11}$$

provided

$$\varepsilon_1 < \Big(\frac{1}{\varepsilon}\Big)^{c\kappa^{-1}}. \tag{3.12}$$

Also, from (3.3') and the preceding

$$|H| > \frac{1}{2}|\Omega| > \frac{\varepsilon}{2}h'. \tag{3.13}$$

Let $\{H_\alpha\}$ be the cosets of $H \subset G$. Then

$$\|1_B * 1_H\|_2^2 = \sum_\alpha \|1_{(B\cap H_\alpha)} * 1_H\|_2^2.$$

Let $\kappa_1 > 0$ be a small parameter and define

$$I_0 = \{\alpha; |B \cap H_\alpha| > (1-\kappa_1)|H|\}$$

and I_1 the complement.

One has

$$\|1_{(B\cap H_\alpha)} * 1_H\|_2^2 = E_+(H, B\cap H_\alpha) \le |B\cap H_\alpha|^2 \cdot |H|$$

and hence, by (3.11)

$$\begin{aligned}(1-c\kappa^{1/12})|B|\cdot|H|^2 &\le |H| \sum |B\cap H_\alpha|^2\\ &\le |H|\Big(\sum_{\alpha\in I_0} |H|\,|B\cap H_\alpha| + (1-\kappa_1)\sum_{\alpha\in I_1} |H|\,|B\cap H_\alpha|\Big)\\ &\le |H|^2(|B| - \kappa_1 \sum_{\alpha\in I_1} |B\cap H_\alpha|).\end{aligned}$$

Hence $B = B_0 \cup B_1$ with

$$|B_1| = \sum_{\alpha\in I_1} |B\cap H_\alpha| < c\kappa^{1/12}\kappa_1^{-1}|B|. \tag{3.14}$$

Assume

$$\kappa \ll \kappa_1^{12} \tag{3.15}$$

so that in particular $I_0 \ne \emptyset$.

Let $y \in A\backslash A_1'$. Then $y \in \Omega$ and by (2.7)

$$|B \cap (B+y)| > (1-\varepsilon_1\varepsilon^{-2})|B|.$$

Let $\varphi : G \to G/H = I_0 \cup I_1$.

If $\alpha \in I_0$, then

$$\begin{aligned}|\big((B\cap H_\alpha)+y\big)\cap B| &\ge |(B+y)\cap B| - \sum_{\alpha'\ne\alpha} |B\cap H_{\alpha'}|\\ &> (1-\varepsilon_1\varepsilon^{-2})|B| - |B| + |B\cap H_\alpha|\\ &> (1-\kappa_1)|H| - \varepsilon_1\varepsilon^{-2}|B|\\ &\underset{(3.13)}{>} (1-\kappa_1-2\varepsilon_1\varepsilon^{-3})|H|.\end{aligned}$$

Thus certainly

$$|H_{\alpha+\varphi(y)} \cap B| > (1-\kappa_1-2\varepsilon_1\varepsilon^{-3})|H|.$$

From (3.14), if $\beta \in I_1$

$$|H_\beta \cap B| < c\kappa^{1/12}\kappa_1^{-1}h \underset{(3.13)}{<} c\kappa^{1/12}\kappa_1^{-1}\varepsilon^{-1}|H|.$$

Assume

$$\varepsilon_1 < 10^{-3}\varepsilon^3 \tag{3.16}$$

and

$$\kappa \ll \kappa_1^{24}\varepsilon^{12} \tag{3.17}$$

Note that the restriction in (3.17) replaces the earlier one in (3.15).

It follows that $|H_\beta \cap B| < \kappa_1|H|$ for $\beta \notin I_0$ while certainly

$$|H_{\alpha+\varphi(y)} \cap B| > \frac{1}{2}|H|.$$

Hence $\alpha + \varphi(y) \in I_0$ and we proved that

$$I_0 + \varphi(y) = I_0 \text{ in } G/H \text{ for all } y \in A\backslash A_1'.$$

Thus

$$\varphi(A\backslash A_1') \subset \text{ Sym}_1(I_0) \text{ in } G/H. \tag{3.18}$$

We distinguish two cases.

If $I_0 = G/H$, then $|B| = |s(A_1')| > (1-\kappa_1)h'$. We may then construct A_1'' as in §2 and conclude (1.8) with $k < (2.4)$, $|\Omega| < \sqrt{\kappa_1}h'$.

Assume next $I_0 \neq G/H$. Hence $\text{Sym}_1(I_0) \neq G/H$ and $H' = \varphi^{-1}\big(\text{Sym}_1(I_0)\big) \supset H$ is a proper subgroup of G. Hence

$$\frac{\varepsilon}{2}h' < |H'| \leq \frac{h'}{2}.$$

By (3.18),

$$A\backslash A_1' \subset H'.$$

Since I_0 is a union of cosets of $\text{Sym}_1(I_0)$ in G/H, $\varphi^{-1}(I_0)$ is a union of cosets H'_τ of H', each satisfying

$$|B \cap H'_\tau| > (1-\kappa_1)|H'| \text{ for } \tau \in I_0'$$

(by definition of I_0), where $I_0 = \bigcup_{\tau \in I_0'} \text{ Sym}_1(I_0)_\tau$.

Thus we may identify H and H' and write

$$A\backslash A_1' \subset H$$

with

$$\frac{\varepsilon}{2}h' < |H| < \frac{h'}{2}. \tag{3.19}$$

The set $s(A_1') = B_0 \cup B_1$ with

$$B_0 = \bigcup_{\alpha \in I_0} \big(s(A_1') \cap H_\alpha\big) \text{ and } B_1 = \bigcup_{\alpha \in I_1} \big(s(A_1') \cap H_\alpha\big)$$

and

$$|s(A_1') \cap H_\alpha| > (1-\kappa_1)|H| \quad \text{for} \quad \alpha \in I_0 \tag{3.20}$$

$$|B_1| < c\kappa^{1/24} h' \tag{3.21}$$

$$I_0 \neq \emptyset, I_0 \neq G/H. \tag{3.22}$$

Next, take a set $z_1, \dots, z_r \in A_1', r < \frac{2}{\varepsilon}$ of representatives for $\varphi(A_1')$ and denote $A_2 = A_1' \backslash \{z_1, \dots, z_r\}$. Then

$$s(A_2) \subset s(A_1') \text{ and } |s(A_2)| \geq 2^{-r}|s(A_1')|.$$

Thus there is some $\alpha \in G/H$ s.t.

$$|s(A_2) \cap H_\alpha| > \frac{\varepsilon}{2}|s(A_2)| > \varepsilon 2^{-r-1}|s(A_1')| > \varepsilon 2^{-r-2} h'.$$

Hence, for each $z \in s(z_1, \dots, z_r)$

$$|s(A_1') \cap H_{\alpha+\varphi(z)}| \geq |\big(s(A_2)+z\big) \cap H_{\alpha+\varphi(z)}| > \varepsilon 2^{-n-2}h'.$$

We claim that $\alpha + \varphi(z) = \beta \in I_0$. Otherwise, $\beta \in I_1$ and $s(A_1') \cap H_\beta \subset B_1$, implying by (3.21) that

$$|s(A_1') \cap H_\beta| < c\kappa^{1/24} h'$$

and this is impossible, provided

$$\kappa < 2^{-\frac{100}{\varepsilon}}. \tag{3.23}$$

Hence

$$I_0 \supset \alpha + \varphi\big(s(z_1, \dots z_r)\big) = \alpha + \varphi\big(s(A_1')\big)$$

and since $I_0 \subset \varphi\big(s(A_1')\big)$, by (3.20), it follows that $I_0 = \varphi\big(s(A_1')\big)$ and therefore by (3.22)

$$\varphi\big(s(A_1')\big) \neq G/H. \tag{3.24}$$

Next partition

$$I_0 = \varphi\big(s(A_1')\big) = J \cup J'$$

with

$$J = \Big\{\alpha \in G/H, |A_1' \cap H_\alpha| > \frac{10}{\varepsilon}\Big\}.$$

Thus

$$\Big|\bigcup_{\alpha \in J'} (A_1' \cap H_\alpha)| < \frac{20}{\varepsilon^2}. \tag{3.25}$$

Take elements $\mathcal{Z} = \big\{z_{\alpha,t}; \alpha \in J, t \leq \frac{10}{\varepsilon}\big\} \cup \{z_\alpha; \alpha \in J'\}$ with $\varphi(z_{\alpha,t}) = \alpha$.

Then

$$s(A_1') \supset s(\mathcal{Z})$$

and

$$\varphi\big(s(A_1')\big) \supset \Big\{\sum_{\alpha \in J} u_\alpha \alpha; 0 \leq u_\alpha \leq \frac{10}{\varepsilon}\Big\} + J' = \langle J \rangle + J'$$

where $\langle J \rangle$ is the group generated by $J \subset G/H$. Thus $|\langle J \rangle| \leq |\varphi\big(s(A_1')\big)|$.

From (3.24), $\langle J\rangle \neq G/H$ and $H' = \varphi^{-1}(\langle J\rangle)$ is a proper subgroup of G.

Hence, by (3.25)

$$|A_1'\backslash H'| < c(\varepsilon) \tag{3.26}$$

and since $A\backslash A_1' \subset H$,

$$|A\backslash H'| < c(\varepsilon)$$

with H' a proper subgroup of G, $[G : H'] \leq \frac{2}{\varepsilon}$.

Recalling the constraints (3.12), (3.15), (3.16), (3.17), (3.23) on the parameters $\varepsilon, \varepsilon_1, \kappa, \kappa_1$, take

$$\kappa_1 = \varepsilon^2$$

$$\kappa = 2^{-\frac{100}{\varepsilon}}$$

$$\varepsilon_1 = \Big(\frac{1}{\varepsilon}\Big)^{C\cdot 2^{\frac{100}{\varepsilon}}}.$$

(4). Summarizing the preceding, we proved the following.

Theorem 1.

Let G be a finite abelian group and $A \subset G, |G| = h'$. Let $\varepsilon > 0$ be a small constant.

There are the following alternatives.

(4.1) $s(A) = G$

(4.2) *There is a proper subgroup H of G, such that*

$$[G : H] < \frac{2}{\varepsilon} \text{ and } |A\backslash H| < c(\varepsilon).$$

(4.3) *There are k elements $x_1, \dots, x_k \in A$ and a subset $\Omega_{x_1,\dots,x_k} \subset G$ depending only on $x_1, \dots, x_k$, such that*

$$k < (1+\varepsilon)\frac{\log h'}{\log 2} + c\log\log h' + c(\varepsilon) \tag{4.4}$$

$$|\Omega_{x_1,\dots,x_k}| \leq \varepsilon h' + k \tag{4.5}$$

and

$$A \subset \Omega_{x_1,\dots,x_k}. \tag{4.6}$$

Again, we note that scenario (4.3) makes up for a very small portion of possible A: if K is the upper bound on k in (4.4) and $|A| \sim m$, there are $\binom{h'}{m}$ total choices for A, and of these at most $\binom{h'}{K} \cdot \binom{\varepsilon h'}{m-K}$ sets A are as in (4.3), which is small compared to the total number of possibilitites for A if ε is small.

§2. Application to the class group

(5). We apply the preceding to the class group $\mathcal{C}$ for a large discriminant $D < 0$.

Let $n \in \mathbb{Z}_+$ be square free; $n = \prod p_j$ with $(p_j, D) = 1$ and $\mathcal{X}_D(p_j) \neq -1$. Let C_j, C_j^{-1} be the classes that represent p_j. Then n is representable by all classes in the formal expansion $\prod\{C_j, C_j^{-1}\}$ (see [Bl], Cor. 2.3).

Let $G = \mathcal{C}^2$. Thus $h' = |G| = h/g$ with $g = |\mathcal{C}/\mathcal{C}^2|$ the number of genera. Let $A = \{C_j^2\} \subset G$. We have

$$\prod\{C_j; C_j^{-1}\} = \Big(\prod C_j^{-1}\Big) s(A) \tag{5.1}$$

with $s(A)$ defined as in (1.0).

Fix $\varepsilon > 0$ a small parameter and apply Theorem 1 to $A \subset G$.

If $s(A) = G$ as in (4.1) of Theorem 1, then

$$\prod\{C_j, C_j^{-1}\} = \Big(\prod C_j^{-1}\Big)\mathcal{C}^2.$$

Since $\mathcal{C}/\mathcal{C}^2$ is the group $\mathcal{G}$ of the genera, it follows that in this case n is representable by any form of the genus if it's representable by some form. Our aim is to show that the alternatives (4.2) and (4.3) of Theorem 1 do not account for many sets $A = \{C_j^2\}$, and in doing so to give lower bounds on the number of integers n which are representable by any form of the genus once they are representable by some form.

Assume now that A satisfies the conditions of alternative (4.2) of Theorem 1.

Denote $\eta : \mathcal{C} \to \mathcal{C}^2$ obtained by squaring and let $\mathcal{C}' = \eta^{-1}(H)$. Since $\mathcal{C}$ is a proper subgroup of $\mathcal{C}_1$, we have

$$\frac{\varepsilon}{2} h < |\mathcal{C}'| \leq \frac{h}{2}$$

where $h = |\mathcal{C}|$ is the class number.

There is a set of indices $\mathcal{J}$ such that $|\mathcal{J}| < C(\varepsilon)$ and for $j \notin \mathcal{J}$, $C_j^2 \in H$, hence $C_j, C_j^{-1} \in \mathcal{C}'$.

Denote $\mathcal{P}_C$ the primes represented by the class C. Thus $\mathcal{P}_C = \mathcal{P}_{C^{-1}}$.

It follows from the preceding that $n\big(\prod_{j\in\mathcal{J}} p_j\big)^{-1}$ has all its prime factors in the set

$$\mathcal{P}(\mathcal{C}') \equiv \bigcup_{C \in \mathcal{C}'} \mathcal{P}_c.$$

We recall the following distributional theorem.

Lemma 2. (Landau; [Bl], Lemma 5.1).

Assume $D < (\log \xi)^A$, A fixed.

Then

$$|\{p \in \mathcal{P}_C; p \leq \xi\}| = \pi_C(\xi) = \frac{1}{\varepsilon(C)h}\int_1^\xi \frac{dt}{\log t} + O(\xi e^{-c\sqrt{\log \xi}}) \tag{5.2}$$

with $\varepsilon(C) = 2$ if C is ambiguous and $\varepsilon(C) = 1$ otherwise.

Recall also that the number of ambiguous classes equals

$$\gamma = \#(\mathcal{C}/\mathcal{C}^2) = \text{number of genera} \ll 2^{\omega(D)}.$$

Hence from (5.2)

$$\pi_{\mathcal{C}'}(\xi) = |\{p \in \mathcal{P}(\mathcal{C}'); p \le \xi\}|$$

$$\le \sum_{C \text{ ambiguous}} \pi_C(\xi) + \frac{1}{2} \sum_{\substack{C \in \mathcal{C}' \\ \text{not ambiguous}}} \pi_C(\xi)$$

$$\le (\gamma + |\mathcal{C}'|) \frac{1}{2h} \int_2^\xi \frac{dt}{\log t} + \mathrm{O}(\xi e^{-c\sqrt{\log \xi}} h)$$

and since $|\mathcal{C}'| \le \frac{h}{2}$ and $h < D^{\frac{1}{2}+\varepsilon} < (\log \xi)^A$

$$< \Big(\frac{1}{4} + \frac{1}{h^{1-\varepsilon}}\Big) \int_2^\xi \frac{dt}{\log t}. \tag{5.3}$$

Thus, in summary, the number of integers $n \le X$ obtained in alternative (4.2), is at most

$$\sum_{\substack{r \le C_\varepsilon; p_1 \dots p_r < X \\ \mathcal{C}' < \mathcal{C} \\ 2 \le [\mathcal{C}; \mathcal{C}'] \le \frac{2}{\varepsilon}}} \#\Big\{n \le \frac{X}{p_1 \dots p_r}; n \text{ square free with prime factors in } \mathcal{P}(\mathcal{C}')\Big\} \tag{5.4}$$

with $\mathcal{P}(\mathcal{C}')$ satisfying (5.3) and $\{p_1, \dots, p_r\}$ unordered and distinct, with $\mathcal{X}_D(p_j) \neq -1$.

To bound the expressions $\#\{\cdots\}$, use the upper bound sieve.

For instance, in the notation of Corollary 6.2 in [I-K], which we apply with $\mathcal{A} = \mathbb{Z}_+$ and

$$P(z) = \prod_{\substack{p \notin \mathcal{P}(\mathcal{C}') \\ p < z}} p \tag{5.5}$$

we have $g(d) = \frac{1}{d}, |r_d(\mathcal{A})| \le 1, \kappa = 1, K = 1$, and

$$V(z) = \prod_{p | p(z)} \big(1 - g(p)\big) = \prod_{\substack{p < z \\ p \notin \mathcal{P}(\mathcal{C}')}} \Big(1 - \frac{1}{p}\Big) \tag{5.6}$$

and from [IK], (6.2), (6.80), applied with $D = z, s = 1$

$$\#\{n < X; \big(n, p(z)\big) = 1\} < CXV(z) + R(z) \tag{5.7}$$

with

$$R(z) = \sum_{d | P(z), d < z} |r_d(\mathcal{A})| \le z. \tag{5.8}$$

Using (5.3) and partial summation

$$\sum_{\substack{p < z \\ p \notin \mathcal{P}(\mathcal{C}')}} \frac{1}{p} > \sum_{u < z} \frac{1}{u^2} |\{p \le u; p \notin \mathcal{P}(\mathcal{C}')\}|$$

$$= \sum_{u < z} \frac{1}{u^2} \Big(\frac{u}{\log u} - \pi_{\mathcal{C}'}(u)\Big) + \mathrm{O}(1)$$

$$> \sum_{\exp(h^{1/A}) < u < z} \Big(\frac{3}{4} - \frac{1}{h^{1-\varepsilon}}\Big) \frac{1}{u \log u} + \mathrm{O}(1)$$

$$> \Big(\frac{3}{4} - \frac{1}{h^{1-\varepsilon}}\Big) \log\Big(\frac{\log z}{h^{1/A}}\Big). \tag{5.9}$$

Hence

$$V(z) \lesssim \exp\left(-\Big(\sum_{\substack{p<z\\ p\notin\mathcal{P}(\mathcal{C}')}} \frac{1}{p}\Big)\right) < \Big(\frac{h^{1/A}}{\log z}\Big)^{\frac{3}{4}-o(1)} \tag{5.10}$$

for $z > \exp(D^{1/A})$.

Let $Y = \frac{X}{p_1\dots p_r}$. Substituting in (5.7) with $z = \sqrt{Y}$ gives for $Y > \exp(D^{1/A})$

$$\#\{n < Y, n \text{ squarefree with prime factors in } \mathcal{P}(\mathcal{C}')\} \lesssim \frac{h^{1/A}}{(\log Y)^{3/4-o(1)}} Y \tag{5.11}$$

(here A is an arbitrary large fixed constant).

Returning to (5.4), we have for $\tau > 0$ fixed, $X^\tau > \exp(D^{1/A})$ that

$$\begin{aligned}
&\sum_{\substack{p_1\dots p_r<X^{1-\tau}\\ \mathcal{X}_D(p_j)\neq 1}} \#\Big\{n \le \frac{X}{p_1\dots p_r}; n \text{ square free with primes in } \mathcal{P}(\mathcal{C}')\Big\}\\
&\overset{(5.11)}{\lesssim} \frac{h^{1/A}X}{\tau(\log X)^{3/4-o(1)}} \sum_{\substack{p_1\dots p_r<X\\ \mathcal{X}_D(p_j)\neq -1}} \frac{1}{p_1\dots p_r}\\
&\lesssim \frac{h^{1/A}X}{\tau(\log X)^{3/4-o(1)}} \frac{(\frac{1}{2}\log\log X)^r}{r!}\\
&\lesssim \frac{h^{1/A}X}{\tau(\log X)^{\frac{3}{4}-o(1)}}
\end{aligned} \tag{5.12}$$

since $r < C(\varepsilon)$.

This gives the contribution

$$\ll \#\Big\{\mathcal{C}' < \mathcal{C}; [\mathcal{C} : \mathcal{C}'] \le \frac{2}{\varepsilon}\Big\}. \frac{h^{o(1)}X}{\tau(\log X)^{\frac{3}{4}-o(1)}}. \tag{5.13}$$

It remains to consider the case $(*)$ in which $n < X$ with prime divisors $p_1, \dots, p_r$ such that $p_1 \dots p_r > X^{1-\tau}$.

Lemma 3. *Fix $r \in \mathbb{Z}_+$. Then, for X large enough*

$$|\{n < X; n \text{ represented by } \mathcal{C} \text{ and product of at most } r \text{ distinct primes}\}|$$
$$< \frac{rX}{\log X}\Big(\frac{e(\frac{1}{2}+\varepsilon)\log\log X}{r-1}\Big)^{r-1}. \tag{5.14}$$

Proof.

We get the estimate

$$\sum_{\substack{p_1<\dots<p_{r-1}\\ \mathcal{X}_D(p_j)\neq -1}} \frac{X(p_1\cdots p_{r-1})^{-1}}{\log(X(p_1\cdots p_{r-1})^{-1})}$$

and since $p_1 \dots p_{r-1} < X^{\frac{r-1}{r}}$, this is

$$< \frac{rX}{\log X} \sum_{\substack{p_1 < \cdots < p_{r-1} < X \\ \mathcal{X}_D(p_j) \neq -1}} \frac{1}{p_1 \cdots p_{r-1}}$$

$$< \frac{rX}{(r-1)! \log X} \Big(\sum_{\substack{p < X \\ \mathcal{X}_D(p) \neq -1}} \frac{1}{p} \Big)^{r-1}. \tag{5.15}$$

From Lemma 2 and partial summation

$$\sum_{\substack{p<X \\ \mathcal{X}_D(p)\neq -1}} \frac{1}{p} = \frac{1}{2} \sum_{C \text{ non-ambiguous}} \sum_{\substack{p \in \mathcal{P}_C \\ p<X}} \frac{1}{p} + \sum_{C \text{ ambiguous}} \sum_{\substack{p \in \mathcal{P}_C \\ p<X}} \frac{1}{p}$$

$$\le (h - |\mathcal{G}|) \Big[\frac{1}{2h} \int^X \frac{1}{y^2} \Big(\int_2^y \frac{dt}{\log t} \Big) dy + c_A \int_{\exp(D^{1/A})}^X \frac{1}{y} \ e^{-c\sqrt{\log y}} dy \Big]$$

$$+ |\mathcal{G}| \Big[\frac{1}{2h} \int^X \frac{1}{y^2} \Big(\int_2^y \frac{dt}{\log t} \Big) dy + C_A \int_{\exp(D^{1/A})}^X \frac{1}{y} \ e^{-\sqrt{\log y}} dy \Big]$$

$$+ \int^{\exp(D^{1/A})} \frac{1}{y^2} \ \frac{y}{\log y} dy$$

$$< \frac{1}{2} \int^X \frac{1}{y^2} \Big(\frac{y}{\log y} + \mathrm{O}\Big(\frac{y}{(\log y)^2} \Big) \Big) dy + C_A h \ e^{-c|D|^{(A/2)}} + \frac{\log |D|}{A}$$

$$< \frac{1}{2} \log\log X + \frac{\log |D|}{A} + \mathrm{O}(1)$$

$$< \Big(\frac{1}{2} + o(1) \Big) \log\log X \tag{5.16}$$

for X large enough.

Substitution of (5.16) in (5.15) gives by Stirling

$$\frac{rX}{\log X} \Big(\frac{e(\frac{1}{2} + \varepsilon) \log\log X}{r-1} \Big)^{r-1}$$

proving Lemma 3. □

Returning to the case $(*)$, we obtain the bound

$$\sum_{\substack{u<X^\tau \\ \text{sq-free represented by } \mathcal{C}}} \frac{rXu^{-1}}{\log X}\Big(\frac{e(\frac{1}{2}+\varepsilon)\log\log X}{r-1}\Big)^{r-1}$$

$$\sim \frac{rX}{\log X}\Big(\frac{e(\frac{1}{2}+\varepsilon)\log\log X}{r-1}\Big)^{r-1}\Big\{\sum_{\substack{u<X^\tau \\ sq \text{ represented by } \mathcal{C}}} \frac{1}{u}\Big\}$$

$$\lesssim \frac{rX}{\log X}\Big(\frac{e(\frac{1}{2}+\varepsilon)\log\log X}{r-1}\Big)^{r-1}\Big(\int^{X^\tau}\frac{h^{1/A}}{u(\log u)^{\frac{1}{2}-o(1)}}+D^{1/A}\Big)$$

$$\lesssim rX\Big(\frac{e(\frac{1}{2}+\varepsilon)\log\log X}{r-1}\Big)^{r-1}\Big(\frac{\sqrt{\tau}}{(\log X)^{\frac{1}{2}-\frac{1}{A}}}+\frac{1}{(\log X)^{1-\frac{1}{A}}}\Big). \tag{5.17}$$

Recall that $r<C_\varepsilon$. Taking $\tau=(\log X)^{-\frac{1}{8}}$, we obtain

$$(5.13)+(5.17)<\#\Big\{\mathcal{C}'<\mathcal{C};[\mathcal{C}:\mathcal{C}']\le\frac{2}{\varepsilon}\Big\}\frac{X}{(\log X)^{\frac{1}{2}+\frac{1}{32}}} \tag{5.18}$$

with ε fixed, $D<(\log X)^C$ and X large enough.

Next, consider the contribution from alternative (4.3) of Theorem 1. This contribution is clearly bounded by

$$\sum_{k \text{ as in } (4.4)}\ \sum_{\substack{p_1<\dots<p_k \\ \mathcal{X}_D(p_j)\neq-1 \\ p_1\dots p_k<X}}\Big|\Big\{n<\frac{X}{p_1\dots p_k};n \text{ square free with primes in } \mathcal{P}\big(\eta^{-1}(\Omega_{p_1,\dots,p_k})\big)\Big\}\Big| \tag{5.19}$$

where $\Omega_{p_1,\dots,p_k}\subset\mathcal{C}^2$ satisfies by (4.5)

$$|\Omega_{p_1\dots p_k}|<2\varepsilon|\mathcal{C}^2|$$

and hence $\tilde\Omega_{p_1\dots p_k}=\eta^{-1}(\Omega_{p_1,\dots,p_k})$ satisfies

$$|\tilde\Omega_{p_1\dots p_k}|<2\varepsilon h. \tag{5.20}$$

Repeating (5.3)-(5.11) with $\mathcal{C}'$ replaced by $\tilde\Omega_{p_1,\dots,p_k}$, we obtain that for $y>\exp(D^{1/A})$

$$|\{n<Y,\ n \text{ square free with prime factors in } \mathcal{P}(\tilde\Omega_{p_1\dots p_k})\}|$$

$$\lesssim \frac{h^{1/A}}{(\log Y)^{1-3\varepsilon}}Y. \tag{5.21}$$

We will consider two cases.

Case 1: Assume $p_1\dots p_k<\sqrt{X}$ in (5.19).

By (5.21), the contribution in (5.19) is bounded above by

$$\frac{h^{1/A}X}{(\log X)^{1-3\varepsilon}} \sum_{\substack{p_1<\cdots<p_k<X \\ \mathcal{X}_D(p_j)=-1}} \frac{1}{p_1\dots p_k}$$

$$< \frac{h^{1/A}X}{(\log X)^{1-3\varepsilon}} \Big(\frac{\frac{e}{2}\log\log X}{k}\Big)^k. \tag{5.22}$$

By (4.4), $k<(1+2\varepsilon)\frac{\log h}{\log 2}$. At this point, the size of h becomes essential. Write $h=(\log X)^\rho$ and $k=\sigma\log\log X$ with $\sigma<\frac{(1+2\varepsilon)}{\log 2}\rho$.

Then (5.22) becomes

$$\frac{h^{1/A}X}{(\log X)^{1-3\varepsilon}}\Big(\frac{e}{2\sigma}\Big)^{\sigma\log\log X} = \frac{h^{1/A}X}{(\log X)^{1-3\varepsilon}}(\log X)^{(1-\log 2\sigma)\sigma}. \tag{5.23}$$

Assume $\kappa>4\varepsilon$ and

$$\rho<(1-\kappa)\frac{\log 2}{2}. \tag{5.24}$$

Then

$$\sigma<\Big(1-\frac{\kappa}{2}\Big)\frac{1}{2}$$

and hence

$$(5.23) < \frac{h^{1/A}X}{(\log X)^{1-3\varepsilon}} \ (\log X)^{\frac{1}{2}(1-\log(1-\frac{\kappa}{2}))(1-\frac{\kappa}{2})}$$

$$< \frac{X}{(\log X)^{1-3\varepsilon-\frac{1}{A}}} \ (\log X)^{\frac{1}{2}-\frac{1}{16}\kappa^2+0(\kappa^3)}$$

$$\leq \frac{X}{(\log X)^{\frac{1}{2}+\frac{\kappa^2}{20}}} \tag{5.25}$$

provided

$$\kappa>10\Big(\sqrt{\varepsilon}+\frac{1}{\sqrt{A}}\Big). \tag{5.26}$$

Case 2: Next, assume in (5.19) that $p_1\dots p_k>\sqrt{X}$. Hence

$$p_k > X^{\frac{1}{2k}}.$$

Rewrite the $p_1,\dots,p_k$ sum in (5.19) as

$$\sum_{\substack{p_1<\cdots<p_{k-1} \\ \mathcal{X}_D(p_j)\neq -1 \\ p_1\cdots p_{k-1}<X^{1-\frac{1}{2k}}}} \ \sum_{X^{\frac{1}{2k}}<p_k<\frac{X}{p_1\cdots p_{k-1}}} \Big|\Big\{n<\frac{X}{p_1\dots p_k}; n \text{ sq-free with primes in } \mathcal{P}(\tilde{\Omega}_{p_1\dots p_k})\Big\}\Big|. \tag{5.27}$$

Fix $p_1\dots p_{k-1}$, and denote $X'=\frac{X}{p_1\cdots p_{k-1}}>X^{\frac{1}{2k}}$.

2a: If $\frac{X}{p_1 \cdots p_k} \leq \exp(|D|^{1/A})$, then $\frac{X'}{\exp D^{1/A}} < p_k < X'$ and we obtain that (5.27) is bounded above by

$$X' \sum_{\frac{X'}{\exp(D^{1/A})} < p_k < X'} \frac{1}{p_k} < X' \{\log\log X' - \log(\log X' - D^{1/A})\}$$

$$\lesssim X' \frac{D^{1/A}}{\log X'} \leq \frac{kX}{p_1 \dots p_{k-1}} \frac{|D|^{1/A}}{\log X} \tag{5.28}$$

2b: If $\frac{X}{p_1 \cdots p_k} > \exp(|D|^{1/A})$, applying (5.21) gives us the upper bound

$$h^{1/A} X' \Big(\sum_{X^{\frac{1}{2k}} < p_k < X'} \frac{1}{(\log \frac{X'}{p_k})^{1-3\varepsilon}} \frac{1}{p_k} \Big) \tag{5.29}$$

for (5.27). Write $2^\ell < \log \frac{X'}{p_k} < 2^{\ell+1}$. Then we have $p_k > X' \cdot e^{-2^\ell}$ and we the inner sum in (5.29) is

$$\lesssim \frac{1}{2^{\ell(1-3\varepsilon)}} [\log\log X' - \log\log(X' e^{-2^\ell})]$$

$$= -\frac{1}{2^{\ell(1-3\varepsilon)}} \log\Big(1 - \frac{2^\ell}{\log X'}\Big). \tag{5.30}$$

Distinguishing between the cases $2^\ell < \frac{1}{2}\log X'$ and $\frac{1}{2}\log X' \leq 2^\ell < \log \frac{X'}{p_k}$ we get

$$(5.30) < \frac{\log\log X}{(\log X')^{1-3\varepsilon}} \lesssim \frac{k \log\log X}{(\log X)^{1-3\varepsilon}} \tag{5.31}$$

and so

$$(5.29) < \frac{k|D|^{1/A}(\log\log X)}{(\log X)^{1-3\varepsilon}} \frac{X}{p_1 \dots p_{k-1}} \tag{5.32}$$

Note that this also captures (5.28).

Substitution of (5.32) in (5.27) gives the bound

$$\frac{k|D|^{1/A}(\log\log X)}{(\log X)^{1-3\varepsilon}} X \Big(\sum_{\substack{p_1 < \cdots < p_{k-1} < X \\ \mathcal{X}_D(p_j) = -1}} \frac{1}{p_1 \dots p_{k-1}} \Big)$$

$$< \frac{(\log\log X)^2 |D|^{1/A}}{(\log X)^{1-3\varepsilon}} X \Big(\frac{\frac{e}{2}\log\log X}{k-1} \Big)^{k-1} \tag{5.33}$$

for which the bound (5.25) on (5.22) holds, under the assumption

$$h < (\log X)^{(1-\kappa)\frac{\log 2}{2}} \tag{5.34}$$

with κ satisfying (5.20).

In view of the preceding, in particular estimates (5.18) and (5.25), and taking into account that $|D|^{\frac{1}{2}-\varepsilon} \ll h \ll |D|^{\frac{1}{2}+\varepsilon}$ and the number of genera is bounded by $2^{\omega(D)} \ll |D|^\varepsilon$, we conclude

Theorem 2. *Let $\kappa > 0$ be a fixed constant and $D < 0$ a negative discriminant satisfying*

$$|D| < (\log X)^{(1-\kappa)\log 2}. \tag{5.35}$$

Let $\mathcal{C}$ be the class group. Then for X large enough

$$\#\{n \sim X; n \text{ square free, representable by some form but not by all forms of the genus}\}$$

$$\lesssim_\kappa \#\Big\{\mathcal{C}' \text{ subgroup of } \mathcal{C}; [\mathcal{C}:\mathcal{C}'] < \frac{10^3}{\kappa^2}\Big\}.\frac{X}{(\log X)^{\frac{1}{2}+\frac{1}{33}}} + \frac{X}{(\log X)^{\frac{1}{2}+\frac{\kappa^2}{20}}}. \tag{5.36}$$

§3. Representation of shifted primes

(6). Next, we establish a version of Theorem 2 for shifted primes.

More precisely we get a bound on

$$\#\{q \sim X \text{ prime}; q+a \text{ square-free and representable by some form but not all of the forms of the genus}\} \tag{6.1}$$

We use a similar strategy, combining the combinatorial Theorem 1 with upper bound sieving, and getting upper bounds on the contributions from alternatives (4.2) and (4.3) of Theorem 1. In fact, only the following crude upper bound will be needed.

Lemma 4. *Let $Y \in \mathbb{Z}$ be a large integer and for each prime $\ell < Y$ let $R_\ell \subset \mathbb{Z}/\ell\mathbb{Z}$ be given*[2]*. Then*

$$\#\{n < Y; \pi_\ell(n) \notin R_\ell \text{ for each } \ell\} < (\log\log Y)^3 \prod_\ell \Big(1 - \frac{|R_\ell|}{\ell}\Big) Y + \frac{Y}{(\log Y)^{10}}. \tag{6.2}$$

Proof.

Denote $\Omega = \{n \in \mathbb{Z}_+; n < Y\}$. and for ℓ prime, let

$$\Omega_\ell = \{n \in \Omega; \pi_\ell(n) \in R_\ell\}$$

Furthermore, for a square-free integer m, write

$$\Omega_m = \bigcap_{\ell | m} \Omega_\ell.$$

We would like to bound

$$\Big|\bigcap_\ell (\Omega \backslash \Omega_\ell)| \le |\bigcap_{\ell < Y_0} (\Omega \backslash \Omega_\ell)| \tag{6.3}$$

with $Y_0 < Y$ to be specified.

[2] $|R_\ell| \in \{0, 1, 2\}$ for the applications that follow.

From the inclusion-exclusion principle

$$(6.3) \leq Y - \sum_{\ell<Y_0} |\Omega_\ell| + \sum_{\ell_1<\ell_2<Y_0} |\Omega_{\ell_1\ell_2}| \ldots + \sum_{\ell_1<\cdots<\ell_r<Y_0} |\Omega_{\ell_1\ldots\ell_r}| \tag{6.4}$$

with $r \in \mathbb{Z}_+$ even to be specified later.

Clearly

$$|\Omega_m| = \Big(\prod_{\ell|m} \frac{|R_\ell|}{\ell}\Big) Y + \mathrm{O}\Big(\prod_{\ell|m} |R_\ell|\Big). \tag{6.5}$$

From (6.4) and (6.5) we have that

$$\frac{(6.3)}{Y} \leq 1 - \sum_{\ell<Y_0} \frac{|R_\ell|}{\ell} + \cdots + \sum_{\ell_1<\cdots<\ell_r<Y_0} \frac{|R_{\ell_1}|}{\ell_1} \cdots \frac{|R_{\ell_r}|}{\ell_r}$$

$$+ \frac{1}{Y}\Big(\sum_{\ell<Y_0} |R_\ell| + \ldots + \sum_{\ell_1<\cdots<\ell_r<Y_0} |R_{\ell_1}| \cdots |R_{\ell_r}|\Big)$$

$$\leq \prod_{\ell<Y_0} \Big(1 - \frac{|R_\ell|}{\ell}\Big) + \sum_{r_1>r} \frac{1}{r_1!}\Big(\sum_{\ell<Y_0} \frac{|R_\ell|}{\ell}\Big)^{r_1} + \frac{2^{r+1}}{Y} \binom{Y_0+r}{r}$$

$$< \exp\Big(3 \sum_{\substack{Y_0<\ell<Y \\ \ell \text{ prime}}} \frac{1}{\ell}\Big) \cdot \prod_{\ell<Y} \Big(1 - \frac{|R_\ell|}{\ell}\Big) + \sum_{r_1>r} \Big(\frac{2e \log\log Y}{r_1}\Big)^{r_1} + (3Y_0)^r Y^{-1}$$

Take $r = 10^2 \log\log Y and Y_0 = Y^{10^{-3}(\log\log Y)^{-1}}$ to obtain (6.2).

Returning to Theorem 1 and alternative (4.2), we have

$$X \sim n = q + a = p_1 \ldots p_r m \tag{6.6}$$

where n is square-free and m has its prime factors in $\mathcal{P}(\mathcal{C}')$. Thus if $\ell \notin \mathcal{P}(\mathcal{C}')$, $\pi_\ell(m) \neq 0$. Let $X' = \frac{X}{p_1 \cdots p_r}$. Since q is prime, we have for any prime $\ell < \frac{X'}{4}, \ell \neq p_1, \ldots p_r$

$$\pi_\ell(m) \neq \pi_\ell(a)/\pi_\ell(p_1 \ldots p_r).$$

Hence we define for $\ell \in \mathcal{P}(\mathcal{C}'), \ell < \frac{X'}{4}, \ell \neq p_1, \ldots, p_r$ the sset R_ℓ by

$$R_\ell = \{\pi_\ell(a)/\pi_\ell(p_1 \ldots p_r)\},$$

and for $\ell \notin \mathcal{P}(\mathcal{C}'), \ell < \frac{X'}{4}, \ell \neq p_1, \ldots, p_r$ the set R_ℓ by

$$R_\ell = \{0, \pi_\ell(a)/\pi_\ell(p_1 \ldots, p_r)\}$$

Otherwise we take $R_\ell = \emptyset$.

Hence, recalling (5.3) and partial summation

$$\sum \frac{|R_\ell|}{\ell} = \sum_{\substack{\ell \in \mathcal{P}(\mathcal{C}') \\ \ell < \frac{X'}{4}}} \frac{1}{\ell} + \sum_{\substack{\ell \notin \mathcal{P}(\mathcal{C}') \\ \ell < \frac{X'}{4}}} \frac{2}{\ell} + \mathrm{O}(\log\log r)$$

$$= 2\log\log X' - \frac{1}{4} \log\log X' + o(\log\log X') \tag{6.7}$$

for $\log X' > (\log X)^{1/A}$.

Therefore, given $p_1 \dots p_r$, the number of possibilities for m in (6.6) is at most

$$\frac{X'}{(\log X')^{7/4-}} \tag{6.8}$$

using (6.2).

Assume $X' > X^\tau$. We obtain the bound (cf. (5.4))

$$\#\Big\{\mathcal{C}' < \mathcal{C}; [\mathcal{C} : \mathcal{C}'] \leq \frac{2}{\varepsilon}\Big\} \cdot \frac{X}{\tau^{7/4}(\log X)^{7/4-}} \cdot \sum_{\substack{p_1<\dots<p_r<X \\ \mathcal{X}_D(p_j)\neq -1, r<C(\varepsilon)}} \frac{1}{p_1\dots p_r}$$

$$< \#\Big\{\mathcal{C}' < \mathcal{C}; [\mathcal{C} : \mathcal{C}'] \leq \frac{2}{\varepsilon}\Big\} \cdot \frac{X}{\tau^{7/4}(\log X)^{7/4-}} \cdot \frac{(\frac{e}{2}\log\log X)^r}{r}$$

$$\ll_\varepsilon \#\Big\{\mathcal{C}' < \mathcal{C}; [\mathcal{C} : \mathcal{C}'] \leq \frac{2}{\varepsilon}\Big\} \cdot \frac{X}{\tau^{3/4}(\log X)^{7/4-}} \tag{6.9}$$

For $X' < X^\tau$, proceed as follows. Since $p_1 < \dots < p_r$ satisfies $p_1 \dots p_r > \sqrt{X}$, we have $p_r > X^{\frac{1}{2r}}$.

Writing

$$n = q + a = p_1 \dots p_{r-1}.p_r \cdot m$$

and denoting $X'' = \frac{X}{p_1\dots p_{r-1}m}$, fix $p_1, \dots, p_{r-1}$, and m and estimate the number of possible $p_r \sim X''$. Thus, for primes $\ell < \frac{1}{4}X''$ such that $(\ell, p_1 \dots p_{r-1}m) = 1$, we have

$$\pi_\ell(p_r) \notin \{0, \pi_\ell(a)/\pi_\ell(p_1 \dots p_{r-1}m)\}$$

and, by Lemma 2, the number of such primes is at most

$$(\log\log X)^4 \frac{X''}{(\log X'')^2} < \frac{r^2 X''}{(\log X)^{2-}}. \tag{6.10}$$

This gives the contribution

$$\sum_{\substack{p_1\dots p_{r-1}m<X \\ m<X^\tau, m \text{ sf} \\ \mathcal{X}_D(p_1),\dots,\mathcal{X}_D(p_{r-1})\neq -1 \\ \mathcal{X}_D(p)\neq -1 \text{ for } p|m}} \frac{X}{p_1\dots p_{r-1}m} \cdot \frac{1}{(\log X)^{2-}} \tag{6.11}$$

$$< \frac{X}{(\log X)^{2-}} \Big(\frac{\frac{e}{2}\log\log X}{r-1}\Big)^{r-1} \Big(\sum_{\substack{m<X^\tau \\ m \text{ sq-free} \\ m \text{representable by } \mathcal{C}}} \frac{1}{m}\Big)$$

$$\overset{(5.11)}{<} \frac{X}{(\log X)^{2-}} \Big(\frac{\frac{e}{2}\log\log X}{r}\Big)^r h^{1/A} \big(\log(X^\tau)\big)^{\frac{1}{2}+}$$

$$< \tau^{1/2} \frac{X}{(\log X)^{\frac{3}{2}-}}. \tag{6.12}$$

to alternative (4.2) if $X' < X^\tau$. Summing (6.9) with the expression in (6.12) we get the total bound

$$\ll_\varepsilon \#\Big\{\mathcal{C}' < \mathcal{C}; [\mathcal{C} : \mathcal{C}'] \le \frac{2}{\varepsilon}\Big\} \frac{X}{(\log X)^{\frac{3}{2}+\frac{1}{20}}} \tag{6.13}$$

for the number of integers $q + a$ which contribute to scenario (4.2) of Theorem 1 (with an appropriate choice of τ).

As before, it remains to consider the contribution of the (4.3) alternative from Theorem 1.

This contribution is again bounded by (5.19), with the additional specification that $n = q + a$ (q prime). Write again

$$X \sim n = q + a = p_1 \dots p_{k-1} p_k m \text{ with } p_1 < \dots < p_k,$$

and recall that $\Omega_{p_1 \dots p_k}$ depends only on the classes $C_1, \dots, C_k \in \mathcal{C}$ determined by $p_1, \dots, p_k$. As before, we have two cases.

Case 1: Assume $p_1 \dots p_k < \sqrt{X}$.

We fix $p_1, \dots, p_k$ and observe that the number of possibilities for m with primes in $\mathcal{P}(\tilde{\Omega}_{p_1,\dots,p_k})$, is at most

$$\frac{X}{p_1 \dots p_{k-1} p_k} \cdot \frac{1}{(\log X)^{2-4\varepsilon}} \tag{6.14}$$

by Lemma 4.

Therefore the contribution in (5.19) in this case is bounded above by

$$\frac{X}{(\log X)^{2-4\varepsilon}} \sum_{\substack{p_1 < \dots < p_k \\ \mathcal{X}_D(p_j) \neq -1}} \frac{1}{p_1 \dots p_k} \tag{6.15}$$

where k again satisfies the condition in (4.4) on Theorem 1. Following the calculations in (5.22) and (5.26), this is bounded above by

$$\frac{X}{(\log X)^{\frac{3}{2}+\frac{\kappa^2}{20}}} \tag{6.16}$$

provided (5.24), i.e.

$$\frac{\log h}{\log \log X} < (1-\kappa) \frac{\log 2}{2}. \tag{6.17}$$

Case 2: Assume $p_1 \dots p_k \ge \sqrt{X}$, so $p_k > X^{\frac{1}{2k}}$.

Proceed as follows.

Fix $p_1, \dots, p_{k-1}$. Then specify the class $\{C, C^{-1}\}$ of (p_k) so that $\tilde{\Omega} = \tilde{\Omega}_{p_1,\dots,p_k}$ is specified. Take m with prime factors in $\mathcal{P}(\tilde{\Omega})$. We are concerned with primes $p = p_k < \frac{X}{p_1 \cdots p_{k-1} m}$ satisfying the conditions

$$p \text{ represented by } C \tag{6.18}$$

$$\pi_\ell(p) \neq \pi_\ell(a)/\pi_\ell(p_1 \dots p_{k-1} m) \text{ if } (\ell, p_1 \dots p_{k-1} m) = 1, \ell < \sqrt{X}. \tag{6.19}$$

and note that the contribution from (4.3) is then bounded above by

$$\sum_{\substack{p_1 < \dots < p_{k-1} \\ \mathcal{X}_D(p_j) \neq -1}} \sum_{C \in \mathcal{C}} \sum_{\substack{m \text{ sq-free with primes in } \mathcal{P}(\tilde{\Omega}) \\ m < \frac{X^{1-\frac{1}{2k}}}{p_1 \cdots p_{k-1}}}} \#\Big\{p \lesssim \frac{X}{p_1 \dots p_{k-1} m}; (6.18), (6,19)\Big\} \tag{6.20}$$

We estimate the number of primes $p = p_k < \frac{X}{p_1 \cdots p_{k-1} m}$ satisfying (6.18) and (6.19) in the following lemma, which we prove later.

Lemma 5. *Let $Y < X$. Then*

$$|\{p < Y, p \text{ satisfies (6.18), (6.19)}\}| \ll \frac{(\log\log X)}{h^{1-\varepsilon}} \; \frac{Y}{(\log Y)^2}. \tag{6.21}$$

From Lemma 5, we have

$$\begin{aligned}\#\Big\{p \lesssim \frac{X}{p_1 \dots p_{k-1} m}; (6.18), (6.19)\Big\} &\ll \frac{k^2 (\log\log X)^4 X}{(\log X)^2 \, p_1 \dots p_{k-1} m \, h^{1-\varepsilon}} \\ &\overset{(4.4)}{\lesssim} \frac{(\log\log X)^6 X}{(\log X)^6 \, p_1 \dots p_{k-1} m \, h^{1-\varepsilon}}.\end{aligned} \tag{6.22}$$

Next, by (5.21),

$$\sum_{\substack{m < \frac{X}{p_1 \cdots p_{k-1}} \\ \text{with primes in } \mathcal{P}(\tilde{\Omega})}} \frac{1}{m} \lesssim h^{1/A} (\log X)^{3\varepsilon}. \tag{6.23}$$

Coming back to (6.20), after summation over $C \in \mathcal{C}$ this gives

$$\begin{aligned}&\frac{h^{\varepsilon+1/A} X}{(\log X)^{2-4\varepsilon}} \sum_{\substack{p_1 < \dots < p_{k-1} < X \\ \mathcal{X}_D(p_j) \neq -1}} \Big(\frac{1}{p_1 \dots p_{k-1}}\Big) < \\ &\frac{X}{(\log X)^{2-5\varepsilon-\frac{1}{A}}} \Big(\frac{\frac{\varepsilon}{2} \log\log X}{k-1}\Big)^{k-1}.\end{aligned} \tag{6.24}$$

Using (6.24) and $k < \frac{1+\varepsilon}{\log 2} \log h$, the assumption (6.17) will again ensure (6.16).

Hence from (6.13), (6.16) and the preceding, we can conclude

Theorem 3. *Let $\kappa > 0$ be a fixed constant and $D < 0$ such that*

$$|D| < (\log X)^{(1-\kappa)\log 2}. \tag{6.25}$$

Let $\mathcal{C}$ be the class group corresponding to D. Then, for X large enough and a fixed positive integer $a = o(X)$, we have

 # $\{q + a \sim X$; q prime, such that $q + a$ is squarefree and representable by some form but not by all forms of the genus$\}$ $\lesssim_\kappa$

$$\#\{\mathcal{C}' \text{ subgroup of } \mathcal{C}; [\mathcal{C} : \mathcal{C}'] < C(\kappa)\} \frac{X}{(\log X)^{\frac{3}{2}+\frac{1}{20}}} + \frac{X}{(\log X)^{\frac{3}{2}+\frac{\kappa^2}{20}}}. \tag{6.26}$$

Note that by decomposing $\mathcal{C}$ into cyclic groups, one easily gets a bound

$$\#\{\mathcal{C}' \text{ subgroup of } \mathcal{C}; [\mathcal{C} : \mathcal{C}'] < C(\kappa)\} < C_1(\kappa)(\log h)^{C_1(\kappa)} < (\log\log X)^{C(\kappa)}.$$

Proof of Lemma 5.

In order to estimate the size of the set

$$\{p < Y, p \text{ satisfies } (6.18),\ (6.19)\} \tag{6.27}$$

we factor in prime ideals and consider the larger set

$$\{\alpha \in I; \alpha \in C, N(\alpha) < Y \text{ and } \pi_\ell\big(N(\alpha)\big) \notin R_\ell \text{ for } \ell < Y_0\} \tag{6.28}$$

where I denotes the integral ideals in $O_K, K = \mathbb{Q}(\sqrt{D}), D = D_0 f^2$ with $D_0 < 0$ squarefree, $N(\alpha)$ stands for the norm of α and ℓ runs over primes,

$$\begin{cases} R_\ell = \{0, \xi_\ell\}, \xi_\ell = \pi_\ell(a)/\pi_\ell(p_1 \dots p_{k-1} m) \text{ if } (\ell, p_1 \dots p_{k-1} m) = 1 \\ R_\ell = \{0\} \text{ otherwise.} \end{cases} \tag{6.29}$$

In fact, we restrict ourselves in (6.28) to primes $\ell < Y$ such that

$$(\ell, p_1 \dots p_{k-1} m) = 1. \tag{6.30}$$

Define

$$\Omega = \{\alpha \in I; \alpha \in C, N(\alpha) < Y\}$$

and

$$\Omega_\ell = \{\alpha \in \Omega; \pi_\ell\big(N(\alpha)\big) \in R_\ell\}$$

for ℓ prime, with

$$\Omega_n = \bigcap_{\ell | n} \Omega_\ell$$

for n square-free.

Proceeding as in the proof of Lemma 4, estimate

$$\Big| \bigcap_{\substack{\ell < Y_0 \\ \ell \text{ satisfies } (6.30)}} (\Omega \backslash \Omega_\ell) \Big| \leq$$

$$|\Omega| - \sum_{\substack{\ell < Y_0 \\ \ell \text{ satisfies } (6.30)}} |\Omega_\ell| + \sum_{\ell_1 < \ell_2 < Y_0} |\Omega_{\ell_1, \ell_2}| - \dots + \sum_{\ell_1 < \dots < \ell_r < Y_0} |\Omega_{\ell_1, \dots, \ell_r}| \tag{6.31}$$

with $r \sim \log\log Y$ a suitably chosen positive integer.

We evaluate $|\Omega_n|$ using Hecke characters.

The condition that $\alpha \in C$ is equivalent to

$$\frac{1}{h} \sum_{\lambda \in \widehat{\mathcal{C}}} \overline{\lambda(C)} \lambda(\alpha) = 1 \tag{6.32}$$

where λ runs over the class group characters $\widehat{\mathcal{C}}$.

Denote $\mathcal{X}_\ell$ the principal character of $\mathbb{Q}(\text{mod}\, \ell)$.

If ℓ satisfies (6.30), the requirement $\pi_\ell\big(N(\alpha)\big) \in R_\ell$ may be expressed as

$$1 - \mathcal{X}_\ell\big(N(\alpha)\big) + \frac{1}{\ell - 1} \sum_{\mathcal{X} (\text{mod}\, \ell)} \overline{\mathcal{X}}(\xi_\ell) \mathcal{X}\big(N(\alpha)\big) = 1. \tag{6.33}$$

Thus

$$|\Omega_n| = \sum_{N(\alpha) < Y} \Big[\frac{1}{h} \sum_{\lambda \in \hat{\mathcal{C}}} \overline{\lambda(C)} \lambda(\alpha)\Big] \prod_{\ell | n} (6.33). \tag{6.34}$$

We will use the following classical extension of the Polya-Vinogradov inequality for finite order Hecke characters.

Proposition 6.

(i) Let $\mathcal{X}$ be a non-principal finite order Hecke character $(\operatorname{mod} f)$ *of K. Then*

$$\Big|\sum_{N(\alpha)<x}\mathcal{X}(\alpha)\Big| < C\big(|D|N(f)\big)^{1/3}[\log|D|N(f)]^2\ x^{1/3} \tag{6.35}$$

and also

(ii)

$$\sum_{N(\alpha)<x} 1 = c_1x + 0\big(|D|^{1/3}(\log|D|)^2\big)x^{1/3} \tag{6.36}$$

where

$$c_1 = \prod_{p|f}\Big(1-\frac{1}{p}\Big)L(1,\mathcal{X}_D\Big). \tag{6.37}$$

This statement follows from [L], (1), (2) p. 479; for (6.37), see [Bl], (2.5).

Analyzing (6.33), (6.34) more carefully, we see that

$$|\Omega_n| = \frac{1}{h}\sum_{N(\alpha)\leq Y}\prod_{\ell|n}\Big(1-\frac{\ell-2}{\ell-1}\mathcal{X}_\ell\big(N(\alpha)\big)\Big) \tag{6.38}$$

$$+\,\mathrm{O}(T_n)$$

where T_n is a bound on sums

$$\sum_{N(\alpha)<Y}\mathcal{X}(\alpha) \text{ with } \mathcal{X}(\alpha) = \lambda(\alpha)\mathcal{X}'\big(N(\alpha)\big) \tag{6.40}$$

where $\lambda\in\hat{\mathcal{C}}, \mathcal{X}'$ is a $(\operatorname{mod} n_1)$-Dirichlet character with $n_1|n$ and either λ or $\mathcal{X}'$ non-principal. By (6.35), we have

$$T_n < C|D|.nY^{1/3} < C|D|Y_0^rY^{1/3} \tag{6.41}$$

so the collected contribution of T_n in (6.31) is at most

$$C|D|Y_0^{2r}Y^{1/3} < Y^{1/2} \tag{6.42}$$

imposing the condition

$$|D|Y_0^r < Y^{\frac{1}{20}}. \tag{6.43}$$

Analyzing further (6.37) using (6.36), we obtain

$$|\Omega_n| = \frac{c_1}{h}\cdot Y\prod_{\substack{\ell|n\\ \mathcal{X}_D(\ell)=1}}\Big[1-\frac{\ell-2}{\ell-1}\Big(1-\frac{1}{\ell}\Big)^2\Big]\cdot\prod_{\substack{\ell|n\\ \mathcal{X}_D(\ell)=0}}\Big[1-\frac{\ell-2}{\ell-1}\Big(1-\frac{1}{\ell}\Big)\Big]\cdot$$

$$\prod_{\substack{\ell|n\\ \mathcal{X}_D(\ell)=-1}}\Big[1-\frac{\ell-2}{\ell-1}\Big(1-\frac{1}{\ell^2}\Big)\Big] + \mathrm{O}(Y^{1/2}) \tag{6.44}$$

Substituting (6.44) in (6.31) gives

$$\frac{c_1}{h} Y \prod_{\substack{\ell < Y_0 \\ \ell \text{ satisfies (6.30)} \\ \mathcal{X}_D(\ell)=1}} \Big(1 - \frac{3}{\ell} + \frac{2}{\ell^2}\Big) \cdot \prod_{\substack{\ell < Y_0 \\ \ell \text{ satisfies (6.30)} \\ \mathcal{X}_D(\ell)=0}} \Big(1 - \frac{2}{\ell}\Big) \cdot \prod_{\substack{\ell < Y_0 \\ \ell \text{ satisfies (6.30)} \\ \mathcal{X}_D(\ell)=-1}} \Big(1 - \frac{1}{\ell} - \frac{2}{\ell^2}\Big) +$$

$$\mathrm{O}\Big(Y \frac{1}{r!}\Big(\sum_{\substack{\ell < Y_0 \\ \ell \text{ prime}}} \frac{3}{\ell}\Big)^r + Y^{1/2} Y_0^r\Big)$$

$$\ll \frac{|D|^\varepsilon}{h} Y \frac{(\log\log X)^3}{(\log Y_0)^2} + \mathrm{O}\Big(Y \Big(\frac{3 \log\log Y_0}{r}\Big)^r + Y^{1/2} Y_0^r\Big). \tag{6.45}$$

Taking $r = 10^2 \log\log Y$ and $Y_0 = Y^{10^{-4}(\log\log Y)^{-1}}$, we have that (6.43) holds and we obtain (6.20). This proves Lemma 5. $\square$

Theorem 3 may be combined with Iwaniec' result [I] on representing shifted primes by the genus of a binary quadratic form (see the Appendix for a quantitative review of that argument, when the quadratic form $Ax^2 + Bxy + Cy^2 = f(x, y)$ is not fixed). Thus, fixing $a \neq 0$, and assuming $D = B^2 - 4AC$ not a perfect square, it follows from [I] that

$$\#\{q + a \sim X; q \text{ prime and } q + a \text{ squarefree and representable by the genus of } f\}$$

$$\gg \frac{X}{(\log X)^{3/2+\varepsilon}} \tag{6.46}$$

and this statement is certainly uniform assuming $|A|, |B|, |C| < \log X$

Corollary 4. *Let f be as above with discriminant $D < 0$, and assume for some $\kappa > 0$*

$$|D| < (\log X)^{(1-\kappa)\log 2} \tag{6.47}$$

with X sufficiently large. Then

$$\#\{q + a \sim X; q \text{ prime, such that } q + a \text{ is representable by } f\}$$

$$\gg \frac{X}{(\log X)^{3/2+\varepsilon}}.$$

Appendix

Let $\phi(x,y)$ be a primitive positive definite binary quadratic form of discriminant $-D$ where $D < \log X$, and let

$$S_1(X,\phi,a) = \sum_{\substack{p\le X, p\nmid D\\ p=f(x,y)+a\\ (x,y)=1, f\in R_\phi}} 1$$

where R_ϕ denotes the genus of ϕ. Then Theorem 1 of [Iw] gives us the following lower bounds for S_1.

Theorem A.1. *For $a \in \mathbb{Z}$ and ϕ a primitive positive definite binary quadratic form of discriminant $-D$ where $D \le \log X$, let $S_1(X,\phi,a)$ be as above. Then for $\epsilon > 0$ we have*

$$S_1(X,\phi,a) \gg_\epsilon \frac{X\cdot D^{-\epsilon}}{(\log X)^{3/2}}$$

where the implied constant does not depend on D.

The following two lemmas are essentially Theorems 2 and 3 from [Iw] in the case $D < \log X$, where the integer m represented by R_ϕ is assumed to be square free and $(m,D) \le 2$.

Lemma A.2. (Iwaniec). *Let $-D < 0$ be the discriminant of $f(x,y) = Ax^2 + 2Bxy + Cy^2$, and write*

$$-D = -2^{\theta_2}\cdot p_1^{\theta_{p_1}}\cdots p_r^{\theta_{p_r}}, \quad D_p = p^{-\theta_p}\cdot D,$$

where $\theta_p \ge 1$ for $1 \le i \le r$, and $\theta_2 \ge 0$. Write $m = \delta n = 2^{\epsilon_2} n$ where m is a positive square free integer (so $0 \le \epsilon_2 \le 1$) such that $(n,2D) = 1$. Then m is represented by the genus of f iff the conditions on m in Table 1 are satisfied[3].

With the notation above, for $p \ne 2$, let

$$\mathcal{L}'_p(n) = \left\{ l \mid 0 < l < p, \left(\frac{l}{p}\right) = \left(\frac{A\cdot 2^{\epsilon_2}}{p}\right)\right\},$$

$$\mathcal{L}''_p(n) = \left\{ l \mid 0 < l < p, \left(\frac{l}{p}\right) = \left(\frac{-A\cdot 2^{\epsilon_2}\cdot k(-D_p)}{p}\right)\right\}$$

[3]Table 1 also specifies a quantity κ and τ for each described case. These do not have to do with whether m is represented or not, but will be used later.

TABLE 1. Representation of $2^{\varepsilon_2}n$ by f

Description of θ_p	$\mathcal{K}$	τ	Contributions on n	Contributions on D	
$\theta_{p_i} \geq 1,\ p_i \neq 2$	$\frac{p_i-1}{2}$	p_i	$\left(\frac{n}{p_i}\right) = \left(\frac{A\cdot 2^{\epsilon_2}}{p_i}\right)$	none	(1)
$p\|m,\ \theta_p = 0$	1	1	none	$\left(\frac{-D}{p}\right) = 1$	(2)
$\epsilon_2 = 0,\ \theta_2 = 0$	1	1	none	$D \equiv -1\ (4)$	(3)
$\epsilon_2 = 0,\ \theta_2 = 2$	1 or 2	4	$n \equiv A\ (4)$ or $n \equiv -A\,D_2\ (4)$	$D_2 \equiv -1\ (4)$ or $D_2 \equiv 1\ (4)$	(4)
$\epsilon_2 = 0,\ \theta_2 = 3$	2	8	$n \equiv A\ (8)$ or $n \equiv A\,(1-2D_2)\ (8)$	none	(5)
$\epsilon_2 = 0,\ \theta_2 = 4$	1	4	$n \equiv A\ (4)$	none	(6)
$\epsilon_2 = 0,\ \theta_2 \geq 5$	1	8	$n \equiv A\ (8)$	none	(7)
$\epsilon_2 = 1,\ \theta_2 = 0$	1	1	none	$D \equiv -1\ (8)$	(8)
$\epsilon_2 = 1,\ \theta_2 = 2$	1	4	$n \equiv A\,\frac{1-D_2}{2}\ (4)$	$D_2 \equiv -1\ (4)$	(9)
$\epsilon_2 = 1,\ \theta_2 = 3$	2	8	$n \equiv -A\,D_2\ (8)$ or $n \equiv A\,(2-D_2)\ (8)$	none	(10)

where $k(-D_p)$ denotes the square free kernel of $-D_p$. Note that each of $\mathcal{L}'_p$ and $\mathcal{L}''_p$ always contains $(p-1)/2$ elements. Define $\mathcal{L}_2(n)$ as follows:

$$\mathcal{L}_2(n) = \begin{cases} \{l \mid 0 < l < 4,\ l \equiv A\ (4) \text{ or } l \equiv -A\,D_2\ (4)\} \text{if } \epsilon_2 = 0,\ \theta_2 = 2 \\ \{l \mid 0 < l < 8,\ l \equiv A\ (8) \text{ or } l \equiv A\,(1-2\,D_2)\ (8)\} \text{if } \epsilon_2 = 0,\ \theta_2 = 3 \\ \{l \mid 0 < l < 4,\ l \equiv A\ (4)\} \text{if } \epsilon_2 = 0,\ \theta_2 = 4 \\ \{l \mid 0 < l < 8,\ l \equiv A\ (8)\} \text{if } \epsilon_2 = 0, \theta_2 \geq 5 \\ \{l \mid 0 < l < 8,\ l \equiv -A\,D_2\ (8) \text{ or } l \equiv A\,(2-D_2)\ (8)\} \text{if } \epsilon_2 = 1, \theta_2 = 3 \\ \{l \mid 0 < l < 4,\ l \equiv -A\,\dfrac{D_2-1}{2}\ (4)\} \text{if } \epsilon_2 = 1, \theta_2 = 2,\ D_2 \equiv -1\ (4) \\ \{0\} \text{if } \epsilon_2 \geq \theta_2. \end{cases}$$

Note that $\mathcal{L}_2(n)$ contains κ elements, where κ is as in Table 1. With this notation, we have

Lemma A.3. (Iwaniec). *Let D, θ_p, m, n, and δ be as in Lemma 0.2, and let τ_2 be the corresponding value of τ in the case $p = 2$ in Table 1. Define $Q = \tau_2 \cdot \prod_{p_i|D_2} p_i$, and let*

$$P = \left\{ p \;\middle|\; \left(\frac{k(-D)}{p}\right) = 1 \right\} \tag{A.1}$$

where $k(-D)$ is the square free kernel of $-D$. Then $m = 2^{\epsilon_2}n$ is represented by the genus of ϕ iff m satisfies the conditions in Table 1, all the prime factors of n belong to P, and

$$n \equiv L\ (Q)$$

where $L > 0$ is an integer satisfying the conditions

- $0 < L < Q$,
- $L \equiv l\ (\tau_2)$ *for some* $l \in \mathcal{L}_2(n)$,
- *for each* $p_i|D_2$ *there exists* $l \in \mathcal{L}'_{p_i}(n)$ *such that* $L \equiv l\ (p_i)$.

Furthermore, if $\mathcal{L}$ denotes the set of L satisfying these conditions, $\left(\frac{k(-D)}{L}\right) = 1$ for each $L \in \mathcal{L}$.

Let $\mathcal{P} = \{\text{primes } p \not| D \text{ s.t. } \left(\frac{k(-D)}{p}\right) = -1\}$, let $E = Q\delta$, and let $\phi_E(N) = \phi(N \cdot E)/\phi(E)$. For D fixed, it is crucial to the $\frac{1}{2}$-dimensional sieve that the condition

$$\left| \sum_{\substack{p \leq z \\ p \in \mathcal{P}}} \frac{\log p}{\phi_E(p)} - \frac{1}{2} \log z \right| < c \tag{A.2}$$

is satisfied for some constant c for all $z > 1$. In our case of $D \leq \log X$, this holds in the following form for some constant C_1 not depending on D:

$$\left| \sum_{\substack{p \leq z \\ p \in \mathcal{P}}} \frac{\log p}{\phi_E(p)} - \frac{1}{2} \log z \right| \ll_\epsilon C_1 D^\epsilon \tag{A.3}$$

for any $z \geq 1$. This can be seen from the proof of Theorem 3.2.1 of [Gl] and the fact that

$$\sum_{\left(\frac{k(-D)}{p}\right)=1, p \leq z} \frac{\log p}{p} = \frac{\log z}{2} + D^\epsilon \cdot O(1)$$

where the implied constant depends only on ϵ. As in [Iw], let

$$C_0 := \lim_{z \to \infty} \prod_{\substack{p < z \\ p \in \mathcal{P}}} \left(1 - \frac{1}{\phi_E(p)}\right) \sqrt{\log z}$$

for which Iwaniec shows in [Iw]

Lemma A.4. (Iwaniec). *Let C_0 be as above. We have*

$$C_0 = e^{-\gamma/2} \prod_{\substack{p \not| a \\ p \in \mathcal{P}}} \left(1 - \frac{1}{(p-1)^2}\right) \cdot \prod_{p | Da} \left(1 - \frac{1}{p}\right)^{-1/2} \cdot \prod_{p \not| Da} \left(1 - \frac{1}{p}\right)^{-\left(\frac{-k(D)}{p}\right)/2}$$

Finally, we recall the following theorem of Bombieri:

Lemma A.5. (Bombieri). *Let $\pi(x, k, l)$ denote the number of primes less than x which are l modulo k. There exists an absolute constant U such that*

$$\sum_{k < \frac{\sqrt{x}}{(\ln x)^U}} \max_{\substack{l \\ (l,k)=1}} \left| \pi(x, k, l) - \frac{\operatorname{Li} x}{\phi(k)} \right| \ll \frac{x}{(\log x)^{20}}.$$

We are now ready to introduce the notation relevant to our problem and recall the lemmas resulting from the $\frac{1}{2}$-dimensional sieve. For L and δ as above, and $1 < s \leq \frac{4}{3}$,

- $D_1 = 2$ or $1 =$ greatest divisor of $2D$ prime to $Q \cdot a$
- $M = \{m \in \mathbb{N} \mid m = \frac{p-a}{\delta}, p \leq X, p \equiv \delta L + a\ (Q\delta),\ (m, D_1) = 1\}$
- $M_d = \{m \in M \mid m \equiv 0\ (d)\}$
- $Y = \phi(E) \cdot |M| = \mathrm{Li}\,(X)$
- $R_d(M) = |M_d| - \frac{Y}{\phi(dE)}$
- $y = \frac{\sqrt{X}}{Q\delta D(\log X)^U}$
- $A(M, y^{1/s}) = \#\{m \in M \,\text{s.t.}\ \ m \not\equiv 0\ (p),\ y^{1/s} > p \in \mathcal{P}\}$

By Lemma A.3, the following is precisely what is needed to evaluate S_1:

$$\begin{aligned} \sum_{\substack{|a|<f(x,y)+a=p\leq X \\ (x,y)=1, f\in R_\phi}} 1 &= \sum_d \sum_{L\in\mathcal{L}} \sum_{\substack{X\geq p\equiv\delta L+a\ (Q\delta) \\ q|((p-a)/\delta)\Rightarrow q\in P \\ ((p-a)/\delta, 2D)=1, p>|a|}} 1 \\ &= \sum_{\substack{\delta \\ 2|a\delta}} \sum_{\substack{L\in\mathcal{L} \\ (\delta L+a, Q\delta)=1}} \sum_{\substack{m\in M \\ q|m\Rightarrow q\in P}} 1 + \mathcal{R} \end{aligned} \tag{A.5}$$

where $\mathcal{R} \leq 2|D|$. It is the innermost sum in (A.5) that we evaluate with the help of the sieve. Note that if $(d, QA) = 1$, there exists an integer d' such that $d'Q + L \equiv 0\ (d)$ and

$$M_d = \{m \mid m = \frac{p+a}{\delta},\ p \leq X\ p \equiv A + \delta\, L + Q\delta\, d'\ (Q\delta\, d)\}.$$

¿From [Iw] we then have

$$\left| |M_d| - \frac{\mathrm{Li}X}{\phi(Q\,\delta d)} \right| \leq 2 \max_{\substack{l \\ (l, Q\,\delta\, d)=1}} \left| \pi(X, Q\delta\, d, l) - \frac{\mathrm{Li}X}{\phi(Q\,\delta\, d)} \right| \tag{A.6}$$

With the notation above, the expression in (A.3) combined with the $\frac{1}{2}$-dimensional sieve gives the following in our case:

Theorem A.6.

$$\begin{aligned} A(M, y^{1/s}) &\gg_\epsilon \sqrt{\frac{e^\gamma}{\pi}} \cdot \frac{C_0 Y}{\phi(E)\sqrt{\log 3y}} \cdot \left(\int_1^s \frac{dt}{\sqrt{t(t-1)}} - \frac{(\log X)^\epsilon}{(\log 3y)^{1/10}} \right) - \sum_{\substack{d<y \\ p|d\Rightarrow p\in\mathcal{P}}} |R_d(M)| \\ &\geq \frac{C_0 \cdot \sqrt{2\frac{e^\gamma}{\pi}}}{\phi(Q\delta)} \cdot \frac{X}{(\log X)^{3/2}} \cdot \left(\int_1^s \frac{dt}{\sqrt{t(t-1)}} + (\log X)^\epsilon \cdot o(1) \right) + \mathrm{O}(X \log^{-20} X). \end{aligned}$$

The estimation of the remainder term comes from Lemma A.5 and (A.6). Also, for sufficiently large X (such that $(X^{1/2}(\log X)^{-15-U})^{1/s} > X^{1/3}$) and $1 < s < \frac{4}{3}$ we have

$$A(M, y^{1/s}) = \sum_{\substack{m\in M \\ q|m\Rightarrow q\in P}} 1 + \sum_{\substack{p_1 p_2 m\in M \\ q|m\Rightarrow q\in P \\ y^{1/s}\leq p_1, p_2\in\mathcal{P}}} 1.$$

We have a lower bound for $A(M, y^{1/s})$, and we would like a lower bound for the first sum in the equation above. To this end, Iwaniec shows:

Lemma A.7. (Iwaniec). *Let* $|Q\delta| \ll (\log X)^{15}$ *and* $s > 1$. *Then*

$$\sum_{\substack{p_1p_2m\in M\\ q|m\Rightarrow q\in P\\ y^{1/s}\le p_1,p_2\in\mathcal{P}}} 1 < \frac{4e^{\gamma/2}C_0\sqrt{s-1}}{\sqrt{\pi}\phi(Q\delta)\sqrt{s}}\log(2s-1)\frac{4s^2X}{(\log X)^{3/2}}(1+o(1))$$

Together with Theorem A.6, for $1 < s < \frac{4}{3}$ and $Q\delta \ll \log X$, this gives us

$$\sum_{\substack{m\in M\\ q|m\Rightarrow q\in P}} 1 \gg \sqrt{\frac{2e^\gamma}{\pi}}\cdot\frac{C_0}{\phi(Q\delta)}\cdot\frac{X}{(\log X)^{3/2}}\cdot\left(\int_1^s \frac{dt}{\sqrt{t(t-1)}} - 8s^2\sqrt{2\frac{s-1}{s}}\log(2s-1)+o(1)\right)+\mathrm{O}(X\log^{-20}X),$$

where the implied constants do not depend on D.

We now compute a lower bound for the expression in (A.5) as in [Iw]. Since D_1 in our case is 1 or 2, the expression Ω_D in (4.8) of [Iw] becomes

$$\Omega_D = c\cdot\sum_{\substack{\delta\\ 2|D\delta}}\sum_{\substack{L\in\mathcal{L}\\ (\delta L+a,Q\delta)=1}}\frac{1}{\phi(Q\delta)} \tag{A.7}$$

where c is a constant not depending on D (coming from the products over $p|D_1$ in (4.8) of [Iw]) and $\delta = 1$ or 2 as in Table 1. Note that the innermost sum of the expression in (4.8) is $\gg_\epsilon D^{-\epsilon}$ for $\epsilon > 0$. This follows from $|\mathcal{L}| = \prod_{p|D_2}(p-1)/2 \gg_{\epsilon'} D^{1-\epsilon'}$. Define

$$\tilde{\Omega}_D = \sum_{\substack{\delta\\ |Q\delta|\le\log^{15}X\\ 2|D\delta}}\sum_{\substack{L\in\mathcal{L}\\ (\delta L+a,Q\delta)=1}}\frac{1}{\phi(Q\delta)}$$

and note that, since $\delta \le 2$ and $D \le \log X$ in our case,

$$\begin{aligned}|\Omega_a - \tilde{\Omega}_a| &\le \sum_{\substack{\delta\\ Q\delta>\log^{15}X\\ p|\delta\Rightarrow p|D}}\frac{Q}{\phi(Q\delta)} < |8D|\cdot\sum_{Q\delta>\log^{15}X}\frac{1}{\sqrt{Q\delta}\sqrt{\phi(Q)}}\\ &< \frac{|8D|}{\log^{7.5}X}\\ &\le \frac{1}{\log^6 X}\end{aligned}$$

Combined with Theorem 1 of [Iw], this gives us the following bounds for $S_1(\phi, X, a)$ where $D \le \log X$ and $\delta = 1$ or 2:

$$\begin{aligned}S_1 &\ge \theta\sqrt{\frac{2e^\gamma}{\pi}}C_0\cdot\tilde{\Omega}_a\frac{X}{(\log X)^{3/2}}(1+o(1)) + \mathrm{O}(X\log^{-20}X)\\ &= \theta\Psi_D\Omega_D\frac{X}{(\log X)^{3/2}}(1+o(1)) + \mathrm{O}(X\log^{-6}X)\end{aligned}$$

where the implied constants do not depend on D,

$$\theta = \sup_{1<s<4/3} \left(\int_1^s \frac{dt}{\sqrt{t(t-1)}} - 8s^2 \sqrt{\frac{2(s-1)}{s}} \log(2s-1) \right),$$

$$C_0 = \Psi_D = \sqrt{\frac{2}{\pi}} \prod_{p|2Da} \left(1 - \frac{1}{p}\right)^{-1/2} \prod_{\substack{p \nmid 2Da \\ \left(\frac{k(-D)}{p}\right)=-1}} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \nmid 2Da} \left(1 - \frac{1}{p}\right)^{-\frac{1}{2}\left(\frac{k(-D)}{p}\right)} \gg_\epsilon D^{-\epsilon}$$

and $\Omega_D \gg_\epsilon D^{-\epsilon}$ as well for $\epsilon > 0$. This gives us the desired generalization of Iwaniec's theorem to Theorem A.1.

References

[Bl]. V. Blomer, *Binary quadratic forms with large discriminants and sums of two squareful numbers*, J. reine angew. Math. (2004), 213–234.

[BF]. J. Bourgain, E. Fuchs,, *A proof of the positive density conjecture for integer Apollonian circle packings*, preprint, http://www.math.ias.edu/ efuchs (2010).

[B-G]. V. Blomer, A. Granville, *Estimates for representation numbers of quadratic forms*, Duke Math. J. Vol. 135, No 2 (2006), 261–302.

[F]. J.J.F. Fournier, *Sharpness in Young's inequality for convolution*, Pacific Journal of Mathematics, Vol. 72, No 2 (1977), 383–397.

[GL]. L. Gelfond, Y. Linnik,, *Elementary methods in analytic number theory*, Moscow (1962).

[Go]. E. Golubeva, *Representation of the large numbers by binary quadratic forms*, J. Math. Sciences, Vol. 89, N 1 (1998), 951–954.

[GW]. B. Green, A. Wigderson, *Lecture notes for the 22nd McGill invitational workshop on computational complexity*, http://www.cs.mcgill.ca/~denis/additive-lectures-v2.pdf.

[I]. H. Iwaniec, *Primes of the type $\varphi(x, y) + A$ where φ is a quadratic form*, Acta Arithmetica, 21 (1972), 203–234.

[I-K]. H. Iwaniec, E. Kowalski, *Analytic Number Theory.*

[L1]. E. Landau, *Über Ideale and Primideale in Idealklassen*, Math. Z. 2 (1916), 52–154.

[L2]. E. Landau, *Verallgemeinerung eines Pólyascher Satzes auf algebraische Zahlkörper.*

[TV]. T. Tao, V. Vu, *Additive combinatorics.*

Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540

Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540