ON REPRESENTATION OF INTEGERS BY BINARY QUADRATIC FORMS

JEAN BOURGAIN AND ELENA FUCHS

ABSTRACT. Given a negative $D > -(\log X)^{\log 2 - \delta}$, we give a new upper bound on the number of square free integers $\ll X$ which are represented by some but not all forms of the genus of a primitive positive definite binary quadratic form of discriminant D. We also give an analogous upper bound for square free integers of the form $q + a \ll X$ 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 $q + a \ll X$ 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 [3], is a lower bound on the number of primes which come up as curvatures in a given primitive integer Apollonian circle packing.

1. 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 [1] and [2]. 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 (we restrict ourselves to discriminants satisfying $\log|D| \leq \mathrm{O}(\log\log X)$).

(i) $|D| \ll (\log X)^{(\log 2)-\varepsilon}$. Then $U_f(X) \gg_{\varepsilon'} X(\log X)^{-\frac{1}{2}-\varepsilon'}$
(ii) $|D| \gg (\log X)^{2(\log 2)+\varepsilon}$. Then $U_f(X) \asymp \frac{X}{\sqrt{D}}$
(iii) The intermediate range.

As Blomer and Granville explain in [2], this transitional behavior is due to the interplay between the size h of the class group $\mathscr{C}$ 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

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

Note that summation of (1) over k gives $\frac{X}{\sqrt{\log X}}$, which corresponds to the number of integers at most X represented by some form of discriminant D.

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 $\mathscr{C}$ that represent the given integer n. Hence, roughly speaking, one would expect that typically n is represented by

The first author was partially supported by NSF Grants DMS-0808042 and DMS-0835373.
The second author was supported by NSF Grant DMS-0635607 and the Simons Foundation.

each class of its genus provided $2^k \gg h$, which amounts to

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

corresponding to alternative (i) since $h = D^{1/2+o(1)}$.

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

$$\frac{2^k}{h} \cdot (1) = \frac{X}{h \log X} \frac{(\log\log X)^{k-1}}{(k-1)!} \tag{3}$$

with total contribution $\mathrm{O}\left(\frac{X}{h}\right)$, attained when $k \sim \frac{1}{2}\log\log X$ (given the precision of the discussion, there is no difference between h and $\sqrt{D}$). This argument corresponds to alternative (ii) above.

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 $n \ll X$, n representable by a form of discriminant D, do actually represent n.

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

Theorem 1.1. *Let D be a negative discriminant satisfying*

$$|D| < (\log X)^{\log 2 - \delta} \tag{4}$$

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

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

$$< \frac{X}{(\log X)^{\frac{1}{2}+\delta'}}. \tag{5}$$

Note that though [1], [2] establish upper and lower bounds for $U_f(X)$ in range (i) – in fact in a more precise form, cf. Theorem 5 in [2] – their results do not directly pertain to the phenomenon expressed in Theorem 1.1. As pointed out in [2], 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

$$D \ll (\log\log X)^{\frac{1}{2}-\varepsilon}. \tag{6}$$

A result in the same spirit was also obtained by Golubeva [6]. Note, however, that even these results of Bernays and Golubeva do not shed light on the situation of shifted primes (with a fixed shift) represented by binary forms, since such integers are themselves a zero-density subset of $\mathbb{Z}$. See Theorem 1.2 for a result in this direction that our methods can prove.

The proof of Theorem 1.1 rests on a general result from arithmetic combinatorics (Theorem 2.1 in Section 2) that we describe next. Assume G a finite abelian group ($G = \mathscr{C}^2$ in our application), $|G| = h'$, in which the group operation will be denoted additively. Given a subset $A \subset G$, we introduce the set

$$s(A) = \left\{ \sum x_i; \{x_i\} \text{ are distinct elements of } A \right\}. \tag{7}$$

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

$$k < (1+\varepsilon)\frac{\log|G|}{\log 2} \tag{8}$$

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

$$|\Omega_{x_1,\dots,x_k}| < \varepsilon|G| \tag{9}$$

(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 (8), and let $|A| \sim m$, where in our application $m \sim K\cdot(1+\alpha)$ for a small fixed $\alpha > 0$, 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 2.1, one applies the greedy algorithm. Thus given $x_1,\dots,x_k \in A$, we select $x_{k+1} \in A$ as to maximize 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 (8), then

$$A \subset \{x_1,\dots,x_k\} \cup \Omega \tag{10}$$

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

$$|s(x_1,\dots,x_k,x)| \approx |s(x_1,\dots,x_k)|. \tag{11}$$

where $\approx$ will be made precise in Section 2. Essentially, adding an element of Ω to $\{x_1,\dots,x_k\}$ will not increase the latter's sum set by much. Assuming Ω fails (9), 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 2.1 is established, deriving Theorem 1.1 is essentially routine. We make use, of course, of Landau's result [11] (established in [1] with uniformity in the discriminant), on the distribution of the primes represented by a given class $C \in \mathscr{C}$ – namely, for $\mathscr{P}_C$ the set of primes represented by a class C,

$$|\{p \in \mathscr{P}_C; p \le \xi\}| = \frac{1}{\varepsilon(C)h}\int_1^{\xi}\frac{dt}{\log t} + C(\xi e^{-c\sqrt{\log\xi}}) \tag{12}$$

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

The nontrivial upper bound (5) is then obtained by excluding certain additional prime divisors, i.e. satisfying $\left(\frac{D}{p}\right) \neq -1$ where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol, 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 1.2. *Under the assumption (4), fixing $a \in \mathbb{Z}$, we have*

$$|\{q+a \ll X;\ q \text{ prime},\ q+a \text{ square free representable by some form of discriminant } D \text{ but not by all forms of the genus}\}| \tag{13}$$
$$< \frac{X}{(\log X)^{\frac{3}{2}+\delta'}}.$$

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 are included in the paper (see Lemmas 3.4 and 3.6), which turned out to be more convenient than searching for a reference. Note that the proof of Lemma 3.6 involves sieving in the ideals

and the required remainder estimates are provided by Landau's extension of the Polya-Vinogradov inequality for Hecke characters [11].

It is worth noting that the motivation behind Theorem 1.2 lies in a result due to H. Iwaniec [8] 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 [3], 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 [3], 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 [8], 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 1.2 for D satisfying (4), while the former is done via a careful analysis of the dependence on the discriminant in [8] for $D < \log X$. This is discussed briefly 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, an appropriate uniform version of Theorem 1 in [8] combined with Theorem 1.2 above implies the following

Corollary 1.3. *Let $D < 0$ satisfy (4) and f be a primitive positive definite binary form of discriminant D. Then*

$$|\{q+a \ll X; q \text{ prime, } q+a \text{ representable by } f\}| \gg \frac{X}{(\log X)^{\frac{3}{2}+\varepsilon}} \tag{14}$$

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

Acknowledgements: The authors are grateful to V. Blomer for several private communications, to B. Green for helpful suggestions on a previous version of this paper, and to the referees for a thorough reading of the paper and for their numerous useful comments.

2. A RESULT IN COMBINATORIAL GROUP THEORY

The aim of this section is to prove Theorem 2.1 below. We will then apply this theorem to the class group in the next section.

For a small constant $\varepsilon > 0$ and an absolute constant C, define $\varepsilon_1, \kappa, \kappa_1$ as follows[1]:

$$\begin{aligned} \kappa_1 &= \varepsilon^2 \\ \kappa &= 2^{-\frac{100}{\varepsilon}} \\ \varepsilon_1 &= \varepsilon^{-C\cdot 2^{\frac{100}{\varepsilon}}}. \end{aligned} \tag{15}$$

Theorem 2.1. *Let G be a finite abelian group with $|G| = h'$ and let $A \subset G$. Denote by*

$$s(A) = \Big\{ \sum x_i;\ \{x_i\} \text{ distinct elements of } A \Big\} \tag{16}$$

the set of sums of distinct elements of A, and let $\varepsilon, \varepsilon_1, \kappa$, and κ_1 be as in (15). There are the following alternatives.

I. $s(A) = G$

II. *There is a proper subgroup H of G (see Lemma 2.2), such that*

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

III. *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*

$$k < (1+\varepsilon)\frac{\log h'}{\log 2} + c \log\log h' + c(\varepsilon) \tag{17}$$

$$|\Omega_{x_1,\dots,x_k}| \le \varepsilon h' + k \tag{18}$$

and

$$A \subset \Omega_{x_1,\dots,x_k}. \tag{19}$$

Again, we note that scenario (III) makes up for a very small portion of possible A: if K is the upper bound on k in (17) 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 (III), which is small compared to the total number of possibilities for A if ε is small.

(1) To prove Theorem 2.1, we start with the following algorithm. Take $x_1 \in A$. Assuming we have obtained $x_1, \dots, x_j$, we take x_{j+1} as to maximize

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

Note that one has

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

Denoting by $\delta_j = \frac{|s(x_1,\dots,x_j)|}{h'}$ the density of $s(x_1,\dots,x_j)$ in G, we therefore have

$$\mathbb{E}_x[|s(x_1,\dots,x_j,x)|] = 2\delta_j h' - \delta_j^2 h' = \delta_j(2-\delta_j)h'. \tag{20}$$

[1] this particular choice of $\varepsilon_1, \kappa, \kappa_1$ will become clear from the necessary constraints (55), (59), (60), (61), (67).

On the other hand, for all x we have

$$|s(x_1,\dots,x_j,x)| \leq (2\delta_j)h'. \tag{21}$$

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

$$\Omega_0 = \{x \in G; |s(x_1,\dots,x_j,x)| < (2-\varepsilon)\delta_j h'\}.$$

Then, from the definition of Ω_0 and (21) we have

$$\mathbb{E}_x[|s(x_1,\dots,x_j,x)|] \leq (2\delta_j h')\Big(1 - \frac{|\Omega_0|}{h'}\Big) + (2-\varepsilon)\delta_j h' \frac{|\Omega_0|}{h'}$$

Together with (20) this implies

$$|\Omega_0| < \frac{\delta_j}{\varepsilon} h'. \tag{22}$$

Note that it follows from (22) that one of the following, (A) or (B), holds.

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

$$|s(x_1,\dots,x_k)| > \varepsilon^2 h' \tag{23}$$

with

$$k < \frac{\log h'}{\log 2 - \frac{\varepsilon}{2}} \tag{24}$$

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

$$A \subset \{x_1,\dots,x_k\} \cup \Omega_{x_1,\dots,x_k} \tag{25}$$

$$k < \frac{\log h'}{\log 2 - \frac{\varepsilon}{2}} \tag{26}$$

$$|\Omega_{x_1,\dots,x_k}| < \varepsilon h'. \tag{27}$$

(2) Suppose the set A satisfies alternative (A) above, and so we obtain $A_1 \subset A$ such that

$$\delta h' = |s(A_1)| > \varepsilon^2 h' \tag{28}$$

Furthermore, suppose $\delta < 1/2$. Fix $\varepsilon_1 > 0$ satisfying (15) and define

$$\Omega_1 = \{x \in G; |s(A_1 \cup \{x\})| < (1-\varepsilon_1)|s(A_1)| + \varepsilon_1 h'\}. \tag{29}$$

Denote by Ω_1^c the complement of Ω_1. If $(A \backslash A_1) \cap \Omega_1^c \neq \emptyset$, we add an element from $(A \backslash A_1) \cap \Omega_1^c$ to A_1 and increase the density from δ in (28) to $(1-\varepsilon_1)\delta + \varepsilon_1$.

Assume this process of adding elements from Ω_1^c can be iterated r times. We then 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

$$r \gg \frac{\log \frac{1}{\varepsilon}}{\varepsilon_1}. \tag{30}$$

We now have $\delta' > 1-\varepsilon^2 > 1/2$. We now define a set Ω_2 for $\{x_1,\dots,x_j\} \subset A$ in the case $\delta_j > 1/2$, where δ_j is as before.

$$\Omega_2 = \{x \in G; |s(x_1,\dots,x_j,x)| < \big(1-(1-\delta_j)^{3/2}\big)h'\}. \tag{31}$$

Similarly to the bound on Ω_0 in (22), we get

$$|\Omega_2| < (1-\delta_j)^{1/2}h'. \tag{32}$$

This set plays a similar role in adding elements to A_1' as Ω_1 did in adding elements to A_1. Consider the set Ω_2 with $\{x_1,\dots,x_j\} = A_1'$ and $\delta_j = \delta'$. Note in particular that $\delta' > 1/2$ implies that $s(A)$ is not a proper subgroup of G. If we replicate the process of adding elements to A_1' from $\Omega_2^c \cap A \backslash A_1'$ as above, we thus obtain a subset $A_1'' \subset A$ so that $s(A_1'') = G$ and

$$|A_1''| \le \frac{\log h'}{(\log 2)-\varepsilon} + c\frac{\log\frac{1}{\varepsilon}}{\varepsilon_1} + \log\log h' \tag{33}$$

unless we are in alternative (B) with (26) replaced by (33). It remains to analyze the case when the iteration on the set A_1 fails.

If $|\Omega_1| < \varepsilon h'$, we are again in the situation (B) with (26) replaced by

$$\frac{\log h'}{\log 2-\varepsilon} + c\frac{\log\frac{1}{\varepsilon}}{\varepsilon_1}. \tag{34}$$

Note that so far the all the alternatives we have analyzed for $s(A)$ are that $s(A) = G$ or that A fits into situation (B) with (26) replaced by (33).

Assume next that Ω_1 defined in (29) satisfies

$$|\Omega_1| > \varepsilon h'. \tag{35}$$

Denoting $B = s(A_1')$, we have by (28) and definition of Ω_1 that

$$|B| > \varepsilon^2 h' \tag{36}$$

Note that, by inclusion-exclusion, for every $x \in \Omega_1$ we have

$$|s(A_1' \cup \{x\})| = |(B+x)\cup B| = |B+x| + |B| - |B\cap(B+x)| = 2\cdot|B| - |B\cap(B+x)|$$

From the definition of Ω_1, we have that $|s(A_1'\cup\{x\})| < (1-\varepsilon_1+\varepsilon_1\varepsilon^{-2})\cdot|B|$, and so

$$|B\cap(B+x)| > (1-\varepsilon_1\varepsilon^{-2})|B| \text{ for } x \in \Omega_1. \tag{37}$$

Hence

$$1_B * 1_{-B} > (1-\varepsilon_1\varepsilon^{-2})|B| \text{ on } \Omega_1 \tag{38}$$

Summing both sides of (38) over $x \in \Omega_1$, we obtain in particular that

$$|B| > (1-\varepsilon_1\varepsilon^{-2})|\Omega_1|. \tag{39}$$

(3) Assume (36)-(39). Thus

$$\langle 1_B, 1_B * 1_{\Omega_1}\rangle = \langle 1_B * 1_{-B}, 1_{\Omega_1}\rangle \ge (1-\varepsilon_1\varepsilon^{-2})|B|\,|\Omega_1| \tag{40}$$

and, noting that $\|1_B\|_2 \cdot \|1_B * 1_{\Omega_1}\|_2 > \langle 1_B, 1_B * 1_{\Omega_1}\rangle$, we have

$$\|1_B * 1_{\Omega_1}\|_2 \ge (1-\varepsilon_1\varepsilon^{-2})|B|^{\frac{1}{2}}|\Omega_1|.$$

Squaring and using the fact that Ω_1 is symmetric, we therefore get

$$\begin{aligned}\langle 1_B * 1_{\Omega_1} * 1_{\Omega_1}, 1_B\rangle &= \langle 1_B * 1_{\Omega_1}, 1_B * 1_{\Omega_1}\rangle \\ &= \|1_B * 1_{\Omega_1}\|_2 \\ &\geq (1-\varepsilon_1\varepsilon^{-2})^2|B|\cdot|\Omega_1|^2\end{aligned}$$

and so we again get

$$\|1_B * 1_{\Omega_1} * 1_{\Omega_1}\|_2 \geq (1-\varepsilon_1\varepsilon^{-2})^2|B|^{\frac{1}{2}}|\Omega_1|^2$$

If we continue squaring, we get that for any given r (= power of 2)

$$\|1_B * 1_{\Omega_1}^{(r)}\|_2 \geq (1-\varepsilon_1\varepsilon^{-2})^r|B|^{\frac{1}{2}}|\Omega_1|^r. \tag{41}$$

(where $1_{\Omega_1}^{(r)}$ denotes the r-fold convolution).

To show that the one other possibility is that A is contained, up to a bounded number of elements, in a proper subgroup H of G of bounded index [G:H] as in (II) of Theorem 2.1, we rely on the following lemma, which is originally due to Fournier [4].

Lemma 2.2. *Let μ be a probability measure on a discrete additive group G. Assume that for small κ as in (15) we have*

$$\|\mu * \mu\|_2 > (1-\kappa)\|\mu\|_2. \tag{42}$$

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

$$\frac{1}{2}\|\mu\|_2^{-2} < |H| < 2\|\mu\|_2^{-2} \tag{43}$$

and for some $z \in G$

$$\Big\|\mu - \frac{1_{H-z}}{|H|}\Big\|_1 < c\kappa^{1/12}. \tag{44}$$

Proof. For $y \in G$, let μ_y denote the push forward of μ when translating by y – i.e. $\mu_y(x) = \mu(x-y)$. From (42) we have

$$\sum_{x\in G}\Big|\sum_{y\in G}\mu(x-y)\mu(y)\Big|^2 > (1-\kappa)^2\|\mu\|_2^2$$

and

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

implying

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

Hence there is $y_0 \in G$ such that

$$\sum_{y\in G}\|\mu_y-\mu_{y_0}\|_2^2\,\mu(y) < 4\kappa\|\mu\|_2^2$$

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

$$\sum_{y\in G}\|\mu_y-\mu\|_2^2\,\mu(y) < 4\kappa\|\mu\|_2^2.$$

Denote

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

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

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

and in particular

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

$$\|\mu\|_2 < \frac{1+4\kappa^{1/3}}{|U|^{1/2}}. \tag{45}$$

Next, write

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

Hence

$$\left\|\mu-\frac{1_U}{|U|}\right\|_2 < \frac{5\kappa^{1/6}}{|U|^{1/2}} \tag{46}$$

and also

$$\begin{aligned}\left\|\mu-\frac{1_U}{|U|}\right\|_1 &\le \mu(U^c)+\sum_{x\in U}\left|\mu(x)-\frac{1}{|U|}\right|\\ &\le 4\kappa^{1/3}+|U|^{1/2}\left\|\mu-\frac{1_U}{|U|}\right\|_2\\ &< 6\kappa^{1/6}. \qquad (47)\end{aligned}$$

From (42), (46), and (47), we have

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

hence

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

where E_+ refers to the additive energy.[2]

We apply now some results from arithmetic combinatorics.

First, by (2.5.4), p.82 from [12] (B-S-G in near-extreme case), there are subsets $U',U''\subset U$ such that

$$|U'|,|U''| > (1-10\kappa^{1/12})|U| \tag{48}$$

[2]It has been pointed out to us by Ben Green that, in fact, from this bound on E_+ the desired result in (44) of Lemma 2.2 follows from Fournier's paper [4], as described in Theorems 1.3.3 and 1.4.6 of notes of Green - Wigderson [7]. We include a different argument based on Kneser's theorem here.

and

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

Thus from Ruzsa's triangle inequality, also

$$|U'-U'|\leq\frac{|U'-U''|^2}{|U''|}<(1+80\kappa^{1/12})|U| \tag{49}$$

Next, we apply Kneser's theorem (see [12], 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

$$|\mathrm{Sym}_1(U'-U')|>(1-80\kappa^{1/12})|U'|. \tag{50}$$

Denote $H=\ \mathrm{Sym}_1(U'-U')$. Note that $H\subset U'-U'$ since $0\in U'-U'$ and thus

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

from (49) and Plunnecke 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 (50)

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

and

$$|U\ \triangle\ (H-z)|<1000\kappa^{\frac{1}{12}}|U|. \tag{51}$$

From (47), (51) we have

$$\left\|\mu-\frac{1_{H-z}}{|H|}\right\|_1<C\kappa^{\frac{1}{12}}. \tag{52}$$

Furthermore, note that by (45), (48), and (50), we have

$$|H|>(1-80\kappa^{1/12})\cdot(1-10\kappa^{1/12})\cdot(1+4\kappa^{1/3})\cdot\|\mu\|_2^{-2}>\frac{1}{2}\|\mu\|_2^{-2}$$

as desired. From (46), (51), we obtain (43) proving Lemma 2.2. □

We now show that the one other alternative for $s(A)$ is alternative (II). Returning to (35) and (41), we have that

$$\left\|\left(\frac{1_{\Omega_1}}{|\Omega_1|}\right)^{(r)}\right\|_2$$

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

$$\log r<\frac{c}{\kappa}\log\frac{1}{\varepsilon} \tag{53}$$

such that $\mu = (\frac{1_{\Omega_1}}{|\Omega_1|})^{(r)}$ satisfies (42) of Lemma 2.2.

From (41), (44), we conclude that

$$\begin{aligned} \left\| 1_B * \frac{1_H}{|H|} \right\|_2 &\geq \big((1-\varepsilon_1\varepsilon^{-2})^r - c\kappa^{1/12}\big)|B|^{1/2} \\ &> (1-c\kappa^{1/12})|B|^{1/2} \end{aligned} \tag{54}$$

provided

$$\varepsilon_1 < \varepsilon^{-c\kappa^{-1}} \tag{55}$$

which we have from the definition of ε_1 in (15). Also, from (43) and the preceding

$$|H| > \frac{1}{2}|\Omega_1| > \frac{\varepsilon}{2}h'. \tag{56}$$

Let $\{H_\alpha\}$ be the set of 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 as defined in (15), and define

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

Let I_1 be the complement of I_0.

One has

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

and hence, by (54)

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

Denote by

$$B_0 = \bigcup_{\alpha\in I_0} \big(B\cap H_\alpha\big) \text{ and } B_1 = \bigcup_{\alpha\in I_1} \big(B\cap H_\alpha\big) \tag{57}$$

Hence $B = B_0 \cup B_1$ with

$$|B_1| = \sum_{\alpha\in I_1} |B\cap H_\alpha| < c\kappa^{1/12}\kappa_1^{-1}|B|. \tag{58}$$

From (15), we have

$$\kappa < c\cdot\kappa_1^{12} \tag{59}$$

with c as in (58), so that in particular $I_0 \neq \emptyset$.

Let $y \in A\backslash A_1'$. Then $y \in \Omega_1$ and by (37)

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

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

If $\alpha \in I_0$, then

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

where the last inequality follows from (56). Thus certainly

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

From (58), if $\beta \in I_1$

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

where the last inequality follows again from (56). From (15, we have

$$\varepsilon_1 < 10^{-3}\varepsilon^3 \tag{60}$$

and

$$\kappa \ll c\cdot\kappa_1^{24}\varepsilon^{12} \tag{61}$$

Note that the restriction in (61) replaces the earlier one in (59).

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

$$\varphi(A\backslash A_1') \subset \ \mathrm{Sym}_1(I_0) \text{ in } G/H. \tag{62}$$

We now distinguish between two cases: $I_0 = G/H$ and $I_0 \neq G/H$.

- 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 (B) with $k <$ (33), $|\Omega_1| < \sqrt{\kappa_1}h'$.
- Assume next $I_0 \neq G/H$. Note that this implies $\mathrm{Sym}_1(I_0) \neq G/H$ and $H' = \varphi^{-1}\big(\mathrm{Sym}_1(I_0)\big) \supset H$ is a proper subgroup of G. Hence
$$\frac{\varepsilon}{2}h' < |H'| \leq \frac{h'}{2}.$$
By (62),
$$A\backslash A_1' \subset H'.$$

Since I_0 is a union of cosets of $\mathrm{Sym}_1(I_0)$ in G/H, we have $I_0' = \varphi^{-1}(I_0)$ 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 $I_0 = \bigcup_{\tau\in I_0'} \mathrm{Sym}_1(I_0)_\tau$.

Thus we may identify H and H' and write

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

with

$$\frac{\varepsilon}{2}h' < |H| < \frac{h'}{2}. \tag{63}$$

The set $s(A_1') = B_0 \cup B_1$ where B_0 and B_1 are as in (57) with B replaced by $s(A_1')$, and we have

- $|s(A_1') \cap H_\alpha| > (1-\kappa_1)|H|$ for $\alpha \in I_0$ (64)
- $|B_1| < c\kappa^{1/24}h'$ (65)
- $I_0 \neq \emptyset$, $I_0 \neq G/H$. (66)

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

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

Thus there is some $\alpha \in G/H$ such that

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

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

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

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 (65) that

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

and this is impossible, provided

$$\kappa < 2^{-\frac{100}{\varepsilon}} \tag{67}$$

which we have by (15). 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 (64), it follows that $I_0 = \varphi\big(s(A_1')\big)$ and therefore by (66)

$$\varphi\big(s(A_1')\big) \neq G/H. \tag{68}$$

Next partition

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

with

$$J = \Big\{\alpha \in G/H, |A_1' \cap H_\alpha| > \frac{10}{\varepsilon}\Big\} \text{ and } J' = I_0 \setminus J.$$

Thus

$$\Big|\bigcup_{\alpha \in J'} (A_1' \cap H_\alpha)| < \frac{20}{\varepsilon^2}. \tag{69}$$

Take elements

$$\mathscr{Z} = \big\{z_{\alpha,t}; \alpha \in J, t \leq \frac{10}{\varepsilon}\big\} \cup \{z_\alpha; \alpha \in J'\}$$

with $\varphi(z_{\alpha,t}) = \alpha$.

Then

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

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

Hence, by (69)

$$|A_1' \backslash H'| < c(\varepsilon) \tag{70}$$

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

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

with H' a proper subgroup of G, $[G:H'] \leq \frac{2}{\varepsilon}$ as in alternative (II) of Theorem 2.1. We have now shown that $s(A)$ must fit into one of the alternatives given in Theorem 2.1. □

Remark: Assume $G = \prod_p G_p$ with $G_p = \prod_{i=1}^k \mathbb{Z}_{p^{\alpha_i}}$, where $k = k(p)$ depends on p. The number of maximal subgroups of G_p is known to be $\frac{p^k-1}{p-1}$ (see [13]). Let $\sigma(G,c)$ denote the number of maximal subgroups H of G such that $[G:H] < c$. Then we have

$$\sigma(G,c) \leq \sum_{p<c} \frac{p^k-1}{p-1} \tag{71}$$

However, without further information on the p-group structure of G, we may only claim a bound $|G|-1$, obtained from the case $G = (\mathbb{Z}/2\mathbb{Z})^k$. Therefore without the information on the p-group structure of G, it is hard to put a meaningful bound the number of subgroups of G satisfying alternative (II) of Theorem 2.1.

3. Application to the class group

In this section, we apply Theorem 2.1 to the class group $\mathscr{C}$ of classes of primitive positive-definite binary quadratic forms of "large" discriminant $D < 0$. Our first application concerns representation of any integers by a given binary form, and our second application is restricted to shifted primes (with a fixed shift) represented by a given binary form, which we recall is of interest, for example, in the context of counting primes in integer Apollonian packings.

3.1. Integers represented by a form.

Let $n \in \mathbb{Z}_+$ be square free; $n = \prod p_j$ with $(p_j, D) = 1$ and $\mathscr{X}_D(p_j) \neq -1$. 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 [1], Cor. 2.3).

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

$$\prod\{C_j; C_j^{-1}\} = \Big(\prod C_j^{-1}\Big) s(A) \tag{72}$$

with $s(A)$ defined as in (16).[3]

Fix $\varepsilon > 0$ a small parameter and apply Theorem 2.1 to $A \subset G$.

If $s(A) = G$ as in (I) of Theorem 2.1, then

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

Since $\mathscr{C}/\mathscr{C}^2$ is the group $\mathscr{G}$ 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 (II) and (III) of Theorem 2.1

[3]For a more detailed discussion of the relationship between the class group and integers represented by binary quadratic forms, see Section 2 of [2].

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.

We start by making a few comments that will greatly simplify the calculations later on.

Lemma 3.1. (i) *Let $0 < \tau < \frac{1}{100}$, and let $\omega(n)$ denote the number of distinct prime factors of n. The number of square free integers $n < X$ with primes in $\mathscr{P}(\mathscr{C})$ and such that*

$$|\omega(n) - \frac{1}{2}\log\log X| > \tau \log\log X \tag{73}$$

is at most

$$\frac{X}{(\log X)^{\frac{1+\tau^2}{2}}} \tag{74}$$

(ii) *Denote by $p_1 > p_2 > \dots$ the prime factors of $n < X$, where n is square free. Let $0 < \gamma < \frac{1}{100}$. The number of square free $n < X$ with primes in $\mathscr{P}(\mathscr{C})$ and such that $\omega(n) \le \gamma$ or*

$$\frac{n}{p_1 \cdots p_r} < X^{\theta} \text{ with } \theta = \min(c^{-r}, \gamma^4) \tag{75}$$

is at most

$$\gamma \cdot \frac{X}{\sqrt{\log X}} \tag{76}$$

Proof. (i) Recalling (1) from Section 1, we obtain the estimate

$$\begin{aligned} & \frac{X}{\log X} \cdot \sum_{|k-\frac{1}{2}\log\log X| > \tau \log\log X} \frac{1}{2^k} \cdot \frac{(\log\log X)^{k-1}}{(k-1)} \\ \ll\ & \frac{X}{\log X} \cdot \left\{ \left(\frac{e}{1-2\tau}\right)^{(\frac{1}{2}-\tau)\log\log X} + \left(\frac{e}{1+2\tau}\right)^{(\frac{1}{2}+\tau)\log\log X} \right\} \\ \ll\ & \frac{X}{\log X} \cdot (\log X)^{\frac{1-\tau^2}{2}} \end{aligned}$$

as desired.

(ii) Write $Y = X^{\theta}$. We may assume $p_1 > \cdots > p_r > Y^{\frac{1}{r}}$, at the cost of replacing Y by Y^2. Note also that $p_1 > \left(\frac{X}{Y}\right)^{1/r} > X^{1/2r}$. Estimate the number of square free $n < X$ as in (ii) of the Lemma by

$$\begin{aligned} & \sum_{\substack{y<Y \\ y \text{ representable}}} \sum_{\substack{p_2\cdots p_r < \frac{X}{Y} \\ p_1 > \cdots > p_r > Y^{1/r}}} 1 \\ \ll\ & \sum_{\substack{y<Y \\ y \text{ representable}}} \sum_{Y^{1/r} < p_2, \dots, p_r < X} \frac{X}{y \cdot p_2 \cdots p_r} \cdot \frac{1}{\log(X^{1/2r})} \\ \ll\ & \frac{2r \cdot X}{\log X} \cdot (\log Y)^{1/2} \cdot \frac{1}{(r-1)} \cdot \left(\log \frac{\log X}{\log(Y^{1/r}}\right)^{r-1} \\ \ll\ & \frac{X}{\log X} \cdot \sqrt{\theta} \cdot r \cdot \left(\frac{e \cdot \log(r\theta^{-1})}{r-1}\right)^{r-1} \\ <\ & \gamma \cdot \frac{X}{\sqrt{\log X}} \end{aligned}$$

as desired where θ satisfies (75) with an appropriate constant c.

□

In view of Lemma 3.1 we see that, given a small $\nu > 0$, all square free integers $n < X$ with primes in $\mathscr{P}(\mathscr{C})$ satisfy

$$|\omega(n) - \frac{1}{2}\log\log X| < \nu \cdot \log\log X \tag{77}$$

and for any given constant r

$$n = p_1 \cdots p_r \cdot y \;\Rightarrow\; y > \exp(\log X)^{1-\nu} \tag{78}$$

outside an exceptional set of size at most

$$\frac{X}{(\log X)^{\frac{1+\nu^2}{2}}} \tag{79}$$

Denote by $\diamondsuit$ the conditions (77) and (78) with $\nu > 0$ some fixed small constant.

Assume now that A satisfies the conditions of alternative (II) of Theorem 2.1. Denote by

$$\eta : \mathscr{C} \to \mathscr{C}^2 \tag{80}$$

the map obtained by squaring and let $\mathscr{C}' = \eta^{-1}(H)$. Since $\mathscr{C}'$ is a proper subgroup of $\mathscr{C}$, we have

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

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

We may assume $\mathscr{C}'$ is a maximal subgroup of $\mathscr{C}$, and the number of such subgroups is at most h as pointed out in the remark at the end of Section 2.

Note that there is a set of indices $\mathscr{J}$ such that $|\mathscr{J}| < C(\varepsilon)$ and for $j \notin \mathscr{J}$ we have $C_j^2 \in H$, hence $C_j, C_j^{-1} \in \mathscr{C}'$. Denote $\mathscr{P}_C$ the primes represented by the class C. Thus $\mathscr{P}_C = \mathscr{P}_{C^{-1}}$.

It follows from the discussion at the beginning of this section that $n\big(\prod_{j\in\mathscr{J}} p_j\big)^{-1}$ has all its prime factors in the set

$$\mathscr{P}(\mathscr{C}') = \bigcup_{C\in\mathscr{C}'} \mathscr{P}_C.$$

We recall the following distributional theorem.

Lemma 3.2 (Landau; [1], Lemma 5.1)**.** *Assume $D < (\log\xi)^A$, A fixed.*

Then

$$|\{p \in \mathscr{P}_C; p \leq \xi\}| = \pi_C(\xi) = \frac{1}{\varepsilon(C)h}\int_1^\xi \frac{dt}{\log t} + O(\xi e^{-c\sqrt{\log\xi}}) \tag{81}$$

with $\varepsilon(C) = 2$ if C is ambiguous[4] *and $\varepsilon(C) = 1$ otherwise.*

Recall also that the number of ambiguous classes equals

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

[4]having order at most 2

Hence from (81) we have

$$\begin{aligned}\pi_{\mathscr{C}'}(\xi) &= |\{p\in\mathscr{P}(\mathscr{C}');p\le\xi\}|\\ &\le \sum_{C\text{ ambiguous}}\pi_C(\xi)+\frac{1}{2}\sum_{\substack{C\in\mathscr{C}'\\ \text{not ambiguous}}}\pi_C(\xi)\\ &= (\gamma_{am}+|\mathscr{C}'|)\frac{1}{2h}\int_2^\xi\frac{dt}{\log t}+\mathrm{O}(\xi e^{-c\sqrt{\log\xi}}h)\end{aligned}$$

and since $|\mathscr{C}'|\le\frac{h}{2}$ and $h<D^{\frac12+\varepsilon}<(\log\xi)^A$ we have

$$\pi_{\mathscr{C}'}(\xi)<\Big(\frac14+\frac{1}{h^{1-\varepsilon}}\Big)\int_2^\xi\frac{dt}{\log t}. \tag{82}$$

Thus, in summary, the number of integers $n\le X$ obtained in alternative (II) of Theorem 2.1 and satisfying $\diamondsuit$ is at most

$$\sum_{\substack{r\le C_\varepsilon;p_1\cdots p_r<X\\ \mathscr{C}'<\mathscr{C}\\ 2\le[\mathscr{C}:\mathscr{C}']\le\frac{2}{\varepsilon}}}\#\Big\{m\le\frac{X}{p_1\cdots p_r};m\cdot p_1\cdots p_r\text{ square free with primes in }\mathscr{P}(\mathscr{C}'),\text{ satisfying }\diamondsuit\Big\} \tag{83}$$

with $\mathscr{P}(\mathscr{C}')$ satisfying (82) and $\{p_1,\dots,p_r\}$ unordered and distinct, such that $\mathscr{X}_D(p_j)\neq-1$.

To bound (83), the number of integers obtained in alternative (II), we proceed as follows. Fix $p_1>\cdots>p_r$ with $r<C_\varepsilon$, and let $Y=\frac{X}{p_1\cdots p_r}$. Note that this satisfies $\log Y>(\log X)^{1-\nu}$ by (78).

Write the prime factorization of m as $m=q_1\cdots q_{r_1}$ with $q_1>\cdots>q_{r_1}$ where $|r_1-\frac12\log\log X|<\nu\cdot\log\log X+C_\varepsilon$ by (77). Thus, fixing $r_1=(\frac12+\sigma)\cdot\log\log X$ with $|\sigma|<2\nu$, we obtain the following bound on the contribution to $\#\{\ \}$ in (83).

$$\begin{aligned}&\sum_{\substack{q_2>\cdots>q_{r_1}\text{ in }\mathscr{P}(\mathscr{C})\\ q_2\cdots q_{r_1}<Y^{1-1/r_1}}}\frac{Y}{q_2\cdots q_{r_1}}\cdot\Big(\log\frac{Y}{q_2\cdots q_{r_1}}\Big)^{-1}\\ &<\ r_1\cdot\frac{Y}{\log Y}\cdot\frac{1}{(r_1-1)}\cdot\Bigg(\sum_{\substack{p\in\mathscr{P}(\mathscr{C}')\\ p<X}}\frac1p\Bigg)^{r_1-1}\end{aligned} \tag{84}$$

By (82) and partial summation,

$$\sum_{p\in\mathscr{P}(\mathscr{C}')}\frac1p=\Big(\frac14+o(1)\Big)\log\log X \tag{85}$$

and therefore

$$\begin{aligned}(84)&<r_1\frac{Y}{\log Y}\big(1+o(1)\big)^{r_1}\Big(\frac{e}{4(\frac12+\sigma)}\Big)^{(\frac12+\sigma)\log\log X}\\ &<r'\big(1+o(1)\big)^{r'}(\log X)^{(\frac12+\sigma)(1-\log2-\log(1+2\sigma))-1+\nu}\frac{X}{p_1\cdots p_r}\end{aligned} \tag{86}$$

where $r'=r_1+r$. Summing over $r_1,p_1>\cdots>p_r$, and $r<C_\varepsilon$ and bounding the number of maximal subgroups $\mathscr{C}'$ of $\mathscr{C}$ trivially by $h<(\log X)^{\frac{\log2}{2}-\delta}$ as before gives the following estimate on (83):

$$\begin{aligned}(83)&<X\cdot(\log X)^{\frac{\log2}{2}-\delta+\varepsilon}(\log\log X)^{C(\varepsilon)}(\log X)^{-\frac12-\frac{\log2}{2}+20\nu}\\ &<\frac{X}{(\log X)^{\frac12+\frac{\delta}{2}}}\end{aligned} \tag{87}$$

for an appropriate choice of $\nu = \nu(\delta)$.

Next, consider the contribution from alternative (III) of Theorem 2.1. This contribution is clearly bounded by

$$\sum_{k \text{ as in (17)}} \sum_{\substack{p_1>\cdots>p_k \\ \chi_D(p_j)\neq -1 \\ p_1\cdots p_k<X}} \Big| \Big\{ m < \frac{X}{p_1\dots p_k}; m \text{ square free with primes in } \mathscr{P}\big(\eta^{-1}(\Omega_{p_1,\dots,p_k})\big) \Big\} \Big| \tag{88}$$

where η is as in (80) and the set $\Omega_{p_1,\dots,p_k} \subset \mathscr{C}^2$ satisfies by (18)

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

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

$$|\tilde{\Omega}_{p_1\dots p_k}| < 2\varepsilon h. \tag{89}$$

Let $Y = \frac{X}{p_1\cdots p_k}$ and let $r = r' - k$ the number of prime factors of m. Again from (81), we obtain

$$\sum_{p \in \mathscr{P}(\tilde{\Omega}_{p_1\dots p_k})} \frac{1}{p} < 2\varepsilon \log\log X. \tag{90}$$

The arguments leading up to (84) give then

$$\begin{aligned} &|\{m < Y; m \text{ square free with prime factors in } \mathscr{P}(\tilde{\Omega}_{p_1\dots p_k})\}| \ll \\ &\frac{Y}{\log Y} \cdot \frac{r}{(r-1)!} \Big(\sum_{\substack{p \in \mathscr{P}(\tilde{\Omega}_{p_1\dots p_k}) \\ p<X}} \frac{1}{p} \Big)^{r-1} \underset{(90)}{<} \frac{Y}{\log Y} (\log X)^{2\varepsilon}. \end{aligned} \tag{91}$$

We distinguish between the following two cases in bounding (88).

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

By (91), the innermost sum in (88) is bounded by

$$\frac{X}{(\log X)^{1-2\varepsilon}} \sum_{\substack{X>p_1>\cdots>p_k \\ \chi_D(p_j)\neq -1}} \frac{1}{p_1\dots p_k} < \frac{X}{(\log X)^{1-3\varepsilon}} \Big(\frac{\frac{e}{2}\log\log X}{k} \Big)^k \tag{92}$$

Case 2. $p_1 \cdots p_k \geq \sqrt{X}$.

Since $p_1 > X^{\frac{1}{2k}}$, we obtain

$$\begin{aligned} &X(\log X)^{2\varepsilon} \cdot \sum_{\substack{X>p_1>\cdots>p_k \\ \chi_D(p_j)\neq -1, p_1>X^{\frac{1}{2k}}}} \frac{1}{p_1\cdots p_k} \frac{1}{\log \frac{X}{p_1\cdots p_k}} < \\ &X(\log X)^{2\varepsilon} \cdot \sum_{\substack{X>p_2>\cdots>p_k \\ \chi_D(p_j)\neq -1}} \frac{1}{p_2\cdots p_k} \sum_{X^{\frac{1}{2k}}<p_1<\frac{X}{p_2\cdots p_k}} \frac{1}{p_1} \frac{1}{\log \frac{X}{p_1 p_2\cdots p_k}} \end{aligned} \tag{93}$$

Since for any Z we have

$$\sum_{X^{\frac{1}{2k}}<p<Z} \frac{1}{p} \frac{1}{\log \frac{Z}{p}} \ll \frac{(\log\log X)^2}{\log X}$$

this gives

$$(93) < \frac{X}{(\log X)^{1-3\varepsilon}} \Big(\frac{\frac{e}{2}\log\log X}{k-1} \Big)^{k-1} \tag{94}$$

similarly to (92).

In evaluating (92), (94), the size of h is essential. Write

$$h = (\log X)^{\rho}, \rho < \frac{\log 2}{2} - \delta$$

and, from (17), $k < (1+2\varepsilon)\frac{\log h}{\log 2} < \sigma \log\log X$ with $\sigma = \frac{(1+2\varepsilon)\rho}{\log 2} < \frac{1}{2} - \frac{\delta}{2}$. Then

$$\begin{aligned}(92),(94) &< \frac{X}{(\log X)^{1-3\varepsilon}} (\log X)^{\frac{1}{2}(1-\delta)(1-\log(1-\delta))} \\ &< \frac{X}{(\log X)^{\frac{1}{2}+\frac{\delta^2}{4}=-3\varepsilon}} \\ &< \frac{X}{(\log X)^{\frac{1}{2}+\frac{1}{5}\delta^2}} \qquad (95)\end{aligned}$$

Recall that $|D|^{\frac{1}{2}-\varepsilon} \ll h \ll |D|^{\frac{1}{2}+\varepsilon}$ and the number of genera is bounded by $2^{\omega(D)} \ll |D|^{\varepsilon}$. In view of (87), (95) and the comments made in the beginning of this section, we proved

Theorem 3.3. *Let $\kappa > 0$ be a fixed constant and $D < 0$ a negative discriminant satisfying*

$$|D| < (\log X)^{(1-\kappa)\log 2}. \qquad (96)$$

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

$$\begin{aligned}&\#\{n \ll X; n \text{ square free, representable by some form but not by all forms of the genus}\} \\ &< \tfrac{X}{(\log X)^{1/2+\kappa'}}\end{aligned}$$

for some $\kappa' = \kappa'(\kappa) > 0$.

3.2. **Representation of shifted primes.** Next, we establish a version of Theorem 3.3 for shifted primes.

More precisely we get a bound on

$$\begin{aligned}&\#\{q \ll X \text{ prime}; q+a \text{ square free and representable by some form but not} \\ &\qquad \text{all of the forms of the genus}\} \qquad (97)\end{aligned}$$

We use a similar strategy based on the combinatorial Theorem 2.1.

Lemma 3.4. *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 where $|R_\ell| \in \{0,1,2\}$. Then*

$$\#\{n < Y; \pi_\ell(n) \notin R_\ell \text{ for each } \ell\} < (\log\log Y)^3 \prod_{\ell} \Big(1 - \frac{|R_\ell|}{\ell}\Big) Y + \frac{Y}{(\log Y)^{10}} \qquad (98)$$

where $\pi_\ell(n)$ denotes the residue class of n mod ℓ.

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

$$\mathscr{Y}_\ell = \{n \in \mathscr{Y}; \pi_\ell(n) \in R_\ell\}$$

Furthermore, for a square free integer m, write

$$\mathscr{Y}_m = \bigcap_{\ell | m} \mathscr{Y}_\ell.$$

We use the bound

$$\Big|\bigcap_{\ell}(\mathscr{Y}\setminus\mathscr{Y}_\ell)|\le|\bigcap_{\ell<Y_0}(\mathscr{Y}\setminus\mathscr{Y}_\ell)| \tag{99}$$

with $Y_0<Y$ to be specified in (102).

From the inclusion-exclusion principle

$$(99)\le Y-\sum_{\ell<Y_0}|\mathscr{Y}_\ell|+\sum_{\ell_1<\ell_2<Y_0}|\mathscr{Y}_{\ell_1\ell_2}|\dots+\sum_{\ell_1<\cdots<\ell_r<Y_0}|\mathscr{Y}_{\ell_1\dots\ell_r}| \tag{100}$$

with an even positive integer $r\in\mathbb{Z}_+$ to be specified in (102).

Clearly

$$|\mathscr{Y}_m|=\Big(\prod_{\ell|m}\frac{|R_\ell|}{\ell}\Big)Y+\mathrm{O}\Big(\prod_{\ell|m}|R_\ell|\Big). \tag{101}$$

From (100) and (101) we have that

$$\begin{aligned}\frac{(99)}{Y} &\le 1-\sum_{\ell<Y_0}\frac{|R_\ell|}{\ell}+\dots+\sum_{\ell_1<\cdots<\ell_r<Y_0}\Big(\frac{|R_{\ell_1}|}{\ell_1}\cdots\frac{|R_{\ell_r}|}{\ell_r}\Big)\\ &+\frac{1}{Y}\Big(\sum_{\ell<Y_0}|R_\ell|+\dots+\sum_{\ell_1<\cdots<\ell_r<Y_0}(|R_{\ell_1}|\cdots|R_{\ell_r}|)\Big)\\ &\le \prod_{\ell<Y_0}\Big(1-\frac{|R_\ell|}{\ell}\Big)+\sum_{r_1>r}\left(\frac{1}{r_1!}\Big(\sum_{\ell<Y_0}\frac{|R_\ell|}{\ell}\Big)^{r_1}+\frac{2^{r+1}}{Y}\binom{Y_0+r}{r}\right)\\ &< \exp\Big(3\cdot\sum_{\substack{Y_0<\ell<Y\\ \ell\text{ prime}}}\frac{1}{\ell}\Big)\cdot\prod_{\ell<Y}\Big(1-\frac{|R_\ell|}{\ell}\Big)+\sum_{r_1>r}\Big(\frac{2e\log\log Y}{r_1}\Big)^{r_1}+(3Y_0)^rY^{-1}\end{aligned}$$

Take

$$r=10^2\log\log Y\ \text{ and }\ Y_0=Y^{10^{-3}(\log\log Y)^{-1}} \tag{102}$$

to obtain the desired bound in (98). □

Similarly to Lemma 3.1, we show below that we may assume $q+a$ satisfies $\diamondsuit$, excluding a set of size at most

$$\frac{X}{(\log X)^{\frac{3}{2}+\nu'}} \tag{103}$$

Lemma 3.5. (i) *Let $\nu>0$ be small. The number of square free integers n of the form $n=q+a, q<X$ prime, with primes in $\mathscr{P}(\mathscr{C})$ and such that*

$$|\omega(n)-\frac{1}{2}\log\log X|>\nu\log\log X \tag{104}$$

is at most

$$\frac{X}{(\log X)^{3/2+\nu'}} \tag{105}$$

for some $\nu'>0$.

(ii) *Denote $p_1>p_2>\cdots$ the prime factors of $n<X$, n square free. The number of $n=q+a$, q prime, with primes in $\mathscr{P}(\mathscr{C})$ and such that either $\omega(n)\le r$ (r a constant) or*

$$\frac{X}{p_1\dots p_r}<\exp(\log X)^{1-\nu} \tag{106}$$

is at most

$$\frac{X}{(\log X)^{3/2+\nu'}} \tag{107}$$

for some $\nu' > 0$.

Proof. (i) Writing $n = q + a = p_1 \dots p_k, p_i \in \mathscr{P}(\mathscr{C})$ and fixing k, we obtain the following bound on the number of square free integers as in (i) of Lemma 3.5:

$$\sum_{\substack{p_2>\cdots>p_r \text{ in } \mathscr{P}(\mathscr{C}) \\ p_2\cdots p_r<X^{1-\frac{1}{r}}}} \Big|\Big\{p < \frac{X}{p_1\cdots p_r}; p\cdot p_2\cdots p_r - a \text{ is prime } \Big\}\Big|. \tag{108}$$

We can assume $r \ll \log\log X$. Let $Y = \frac{X}{p_2\cdots p_r}$. By Lemma 3.4,

$$\begin{aligned} |\{p < Y; pp_2\dots p_r - a \text{ is prime}\}| &\ll (\log\log X)^3 \cdot \frac{Y}{(\log Y)^2} \\ &\ll (\log\log X)^5 \cdot \frac{Y}{(\log X)^2}. \end{aligned} \tag{109}$$

Substituting (109) in (108) gives

$$\begin{aligned} & X\cdot(\log\log X)^5(\log X)^{-2}\cdot \sum_{\substack{X>p_2>\cdots>p_r \\ p_2,\cdots,p_r \text{ in } \mathscr{P}(\mathscr{C})}} \frac{1}{p_2\dots p_r} \\ & < X\cdot(\log\log X)^5\cdot(\log X)^{-2}\cdot\Big(\frac{\log\log X}{2}\Big)^{r-1}\cdot\frac{1}{(r-1)!} \end{aligned} \tag{110}$$

the contribution of (110) for r satisfying (104) is at most (105) as desired.

(ii) Letting $Y = \exp(\log X)^{1-\nu}$, we obtain

$$\begin{aligned} & \sum_{\substack{y<Y \\ y \text{ with primes in } \mathscr{P}(\mathscr{C})}} \sum_{\substack{p_1\cdots p_r<\frac{X}{y} \\ p_1>\cdots>p_r>Y^{1/r} \\ p_1\cdots p_r\cdot y+a \text{ prime}}} 1 \\ & \ll \sum_{\substack{y<Y \\ y \text{ repr.}}} \sum_{Y^{1/r}<p_2,\dots,p_r<X} \Big|\Big\{p < \frac{X}{y\cdot p_2\cdots p_r}; p\cdot p_2\cdots p_r y + a \text{ prime}\Big\}\Big| \\ & \ll \sum_{\substack{y<Y \\ y \text{ repr.}}} \sum_{Y^{1/r}<p_2,\dots,p_r<X} (\log\log X)^5(\log X)^{-2}\frac{X}{y\cdot p_2\cdots p_r} \\ & \ll (\log\log X)^5(\log X)^{-2}(\log Y)^{\frac{1}{2}}X\Big(\log\frac{r\log X}{\log Y}\Big)^{r-1}\frac{1}{(r-1)!} \\ & \ll (\log\log X)^{r+5}\frac{X}{(\log X)^{\frac{3}{2}+\frac{\nu}{3}}} \\ & < \frac{X}{(\log X)^{\frac{3}{2}+\frac{\nu}{3}}} \end{aligned} \tag{111}$$

and hence we get (107) as desired.

□

Returning to Theorem 2.1 and alternative (II), we have

$$X \gg n = q + a = p_1 \dots p_r m \tag{112}$$

where n is square free and m has its prime factors in $\mathscr{P}(\mathscr{C}')$.

Proceeding as in the proof of Theorem 1.1, estimate the contribution to (II) by

$$\sum_{\substack{r\le C_\varepsilon; X>p_1>\cdots>p_r\\ \mathscr{C}'<\mathscr{C}}} \Big|\Big\{m<\frac{X}{p_1\dots p_r}; m \text{ as above and } p_1\cdots, p_r\cdot m \text{ satisfying } \diamondsuit\Big\}\Big| \tag{113}$$

Let $Y=\frac{X}{p_1\cdots p_r}$ and write $m=q_1\dots q_{r_1}$, with $q_1>\cdots>q_{r_1}$ the prime factorization of m, where $|r_1-\frac{1}{2}\log\log X|<\nu\log\log X$ by assumption $\diamondsuit$.

Thus, after fixing r_1 we have that

$$|\{\cdots\}| \text{ in (113)} \le \sum_{\substack{q_2>\cdots>q_{r_1} \text{ in } \mathscr{P}(\mathscr{C}')\\ q_2\cdots q_{r_1}<Y^{1-\frac{1}{r_1}}}} (*) \tag{114}$$

where

$$\begin{aligned}(*)&=\Big|\Big\{p<\frac{Y}{q_2\dots q_{r_1}}; p_1\cdots p_r\cdot q_2\cdots q_{r_1}\cdot p-a \text{ prime}\Big\}\Big|\\ &\overset{\text{Lemma 3.4}}{\ll} (\log\log X)^3\frac{Y}{q_2\cdots q_{r_1}}\Big(\log\frac{T}{q_2\cdots q_{r_1}}\Big)^{-2}\\ &\ll (\log\log X)^5\frac{1}{(\log X)^{2(1-\nu)}}\cdot\frac{Y}{q_2\cdots q_{r_1}} \qquad (115)\end{aligned}$$

since $\log Y>(\log X)^{1-\nu}$ and $\frac{Y}{q_2\cdots q_{r_1}}>Y^{\frac{1}{r_1}}$.

Thus

$$\begin{aligned}(114)&\ll Y\frac{\log\log X)^5}{(\log X)^{2(1-\nu)}}\sum_{X>q_2>\cdots>q_{r_1} \text{ in } \mathscr{P}(\mathscr{C}')}\frac{1}{q_2\cdots q_{r_1}}\\ &\ll Y\frac{(\log\log X)^5}{(\log X)^{2(1-\nu)}}\cdot\frac{1}{(r_1-1)!}\Big(\sum_{\substack{p\in\mathscr{P}(\mathscr{C}')\\ r<X}}\Big)^{r_1-1} \qquad (116)\end{aligned}$$

Writing $r_1=(\frac{1}{2}+\sigma)\log\log X$ where $|\sigma|<\nu$,

$$(116)\ll\frac{\log\log X)^5}{(\log X)^{2(1-\nu)}}(\log X)^{(\frac{1}{2}+\sigma)(1-\log 2-\log(1+2\sigma))+\varepsilon}\frac{X}{p_1\cdots p_r}. \tag{117}$$

Summing over r_1; $p_1>\cdots>p_r, r<C_\varepsilon$; and the maximal subgroups $\mathscr{C}'$ of $\mathscr{C}$ gives

$$(113)<h\frac{X}{(\log X)^{2-2\nu}}(\log X)^{\frac{1}{2}-\frac{\log 2}{2}+O(\sigma)}.$$

Assuming $h<(\log X)^{\frac{\log 2}{2}-\delta}$, we obtain

$$(113)<\frac{X}{(\log X)^{\frac{3}{2}+\delta-2\nu-0(\sigma)}}<\frac{X}{(\log X)^{\frac{3}{2}+\frac{\delta}{2}}} \tag{118}$$

for an appropriate choice of ν.

Next, we analyze the contribution of alternative (III) from Theorem 2.1 in the case of shifted primes.

This contribution is again bounded by (88), with the additional specification that $n=q+a$ (q prime). Write again

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

and recall that $\Omega_{p_1\dots p_k}$ depends only on the classes $C_1,\dots,C_k\in\mathscr{C}$ determined by $p_1,\dots,p_k$. We again have the following two cases.

Case 1: Assume first that $p_1\dots p_k<\sqrt{X}$ and estimate

$$\sum_{k \text{ as in (17)}} \sum_{\substack{p_k>\cdots>p_1\\ \chi_D(p_j)\neq -1\\ p_1\cdots p_k<\sqrt{X}}} \Big|\Big\{m<\frac{X}{p_1\dots p_k};\quad \begin{array}{l} p_1\dots p_k m-a \text{ prime}\\ m \text{ square free with factors in } \mathscr{P}(\tilde{\Omega}_{p_1\dots p_k})\end{array}\Big\}\Big|. \tag{119}$$

where $\tilde{\Omega}_{p_1\dots p_k}=\eta^{-1}(\Omega_{p_1,\dots,p_k})$. Let $Y=\frac{X}{p_1\cdots p_k}$ and let $m=q_1\cdots q_{r_1}$ be the prime factorization of m, where $q_1>\cdots>q_{r_1}$ and $r'=k+r_1$ satisfies $|r'-\frac{1}{2}\log\log X|<\nu\log\log X$. Thus certainly $r_1<\log\log X$. Fix r_1 and note that $|\{\cdots\}|$ in (119) is

$$\leq \sum_{\substack{q_2>\cdots>q_{r_1} \text{ in } \mathscr{P}(\tilde{\Omega})\\ q_2\cdots q_{r_1}<Y^{1-\frac{1}{r_1}}}} (**) \tag{120}$$

where

$$\begin{aligned}(**)&=\Big|\Big\{p<\frac{Y}{q_2\cdots q_{r_1}}; p_1\cdots p_{k-1}\cdot q_2\cdots q_{r_1}\cdot p-a \text{ prime}\Big\}\Big|\\ &\ll (\log\log X)^5\frac{Y}{(\log Y)^2}\ \frac{1}{q_2\cdots q_{r_1}}.\end{aligned} \tag{121}$$

Since

$$\sum_{p\in\mathscr{P}(\tilde{\Omega})}\frac{1}{p}<2\varepsilon\log\log X$$

this gives

$$\begin{aligned}(120)&\ll(\log\log X)^5\frac{1}{(r_1-1)!}(2\varepsilon\log\log X)^{r_1-1}\ \frac{Y}{(\log Y)^2}\\ &<(\log X)^{3\varepsilon}\frac{Y}{(\log X)^2}\end{aligned} \tag{122}$$

since $Y>\sqrt{X}$. Hence (119) is bounded by

$$\frac{X}{(\log X)^{2-3\varepsilon}}\sum_{\substack{X>p_1>\cdots>p_2\\ \chi_D(p_j)\neq -1}}\frac{1}{p_1\cdots p_k}<\frac{X}{(\log X)^{2-3\varepsilon}}\Big(\frac{\frac{e}{2}\log\log X}{k}\Big)^k. \tag{123}$$

In view of (17) and the assumption on $h<(\log X)^{\frac{\log 2}{2}-\delta}$, we conclude similarly as in the proof of Theorem 3.3 that

$$(123)<\frac{X}{(\log X)^{\frac{3}{2}+\frac{1}{5}\delta^2}}. \tag{124}$$

Case 2: Assume $p_1\cdots p_k\geq\sqrt{X}$. In particular, since $p_1<p_2<\cdots<p_k$, we have that $p_k>X^{\frac{1}{2k}}$. The argument given above for $p_1\cdots p_k<\sqrt{X}$ may not be conclusive anymore and so we adopt a variant of the previous approach.

Proceed as follows.

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

the conditions

$$\bullet\ p \text{ represented by } C \tag{125}$$

$$\bullet\ \pi_\ell(p) \neq \pi_\ell(a)/\pi_\ell(p_1\dots p_{k-1}m) \text{ if } (\ell, p_1\dots p_{k-1}m) = 1, \ell < \sqrt{X}. \tag{126}$$

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

$$\sum_{\substack{p_1<\dots<p_{k-1}\\ \mathscr{X}_D(p_j)\neq -1}} \sum_{C\in\mathscr{C}} \sum_{\substack{m \text{ sq-free with primes in } \mathscr{P}(\tilde{\Omega})\\ m<\frac{X^{1-\frac{1}{2k}}}{p_1\cdots p_{k-1}}}} \#\Big\{p \ll \frac{X}{p_1\cdots p_{k-1}\cdot m};\ p \text{ satisfying (125), (126)}\Big\} \tag{127}$$

We estimate the number of primes $p = p_k < \frac{X}{p_1\cdots p_{k-1}\cdot m}$ satisfying (125) and (126) in the following lemma, which we prove later.

Lemma 3.6. *Let $Y < X$. Then*

$$|\{p < Y, p \text{ satisfies (125), (126)}\}| \ll \frac{(\log\log X)^5}{h^{1-\varepsilon}} \cdot \frac{Y}{(\log Y)^2}. \tag{128}$$

From Lemma 3.6, we have

$$\begin{aligned} \#\Big\{p \ll \frac{X}{p_1\cdots p_{k-1}\cdot m};\ p \text{ satisfying (125), (126)}\Big\} &\ll \frac{k^2(\log\log X)^5 X}{(\log X)^2\, p_1\cdots p_{k-1}\cdot m h^{1-\varepsilon}} \\ &\ll \frac{(\log\log X)^7 X}{(\log X)^2\, p_1\cdots p_{k-1}\cdot m h^{1-\varepsilon}}. \end{aligned} \tag{129}$$

Next, by (90),

$$\sum_{\substack{m<\frac{X}{p_1\cdots p_{k-1}}\\ \text{with primes in } \mathscr{P}(\tilde{\Omega})}} \frac{1}{m} \ll (\log X)^{3\varepsilon}. \tag{130}$$

Coming back to (127), after summation over $C \in \mathscr{C}$ this gives again

$$\begin{aligned} &\frac{h^\varepsilon X}{(\log X)^{2-4\varepsilon}} \sum_{\substack{p_1<\dots<p_{k-1}<X\\ \mathscr{X}_D(p_j)\neq -1}} \Big(\frac{1}{p_1\cdots p_{k-1}}\Big) \\ <\ &\frac{X}{(\log X)^{2-5\varepsilon}} \Big(\frac{\frac{e}{2}\log\log X}{k-1}\Big)^{k-1} \\ <\ &\frac{X}{(\log X)^{3/2+\delta^2/5}} \end{aligned}$$

by the bound on k in (17), as well as the assumption on h.

Hence from the preceding, we can conclude

Theorem 3.7. *Let $\kappa > 0$ be a fixed constant and $D < 0$ such that*

$$|D| < (\log X)^{(1-\kappa)\log 2}. \tag{131}$$

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

$$\begin{aligned} &\#\{q+a \ll X;\ q \text{ prime, } q+a \text{ square free and representable by some form but not by all forms of the genus}\} \\ &\qquad < \frac{X}{(\log X)^{3/2+\kappa'}} \end{aligned} \tag{132}$$

for some $\kappa' = \kappa'(\kappa) > 0$.

Proof of Lemma 3.6.

In order to estimate the size of the set

$$\{p < Y, p \text{ satisfies (125), (126)}\} \tag{133}$$

we factor in prime ideals and consider the larger set

$$\{\alpha \in I; \alpha \in C, N(\alpha) < Y \text{ and } \pi_\ell\big(N(\alpha)\big) \notin R_\ell \text{ for } \ell < Y_0\} \tag{134}$$

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

$$\begin{cases} R_\ell = \{0, \xi_\ell\}, \xi_\ell = \pi_\ell(a)/\pi_\ell(p_1 \cdots p_{k-1} \cdot m) \text{ if } (\ell, p_1 \cdots p_{k-1} \cdot m) = 1 \\ R_\ell = \{0\} \text{ otherwise.} \end{cases} \tag{135}$$

In fact, we restrict ourselves in (134) to primes $\ell < Y$ such that

$$(\ell, \alpha \cdot p_1 \cdots p_{k-1} \cdot m) = 1. \tag{136}$$

Define

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

and

$$\mathscr{Y}_\ell = \{\alpha \in \mathscr{Y}; \pi_\ell\big(N(\alpha)\big) \in R_\ell\}$$

for ℓ prime,

$$\mathscr{Y}_n = \bigcap_{\ell | n} \mathscr{Y}_\ell$$

for n square free.

Proceeding as in the proof of Lemma 3.4, estimate

$$\Big| \bigcap_{\substack{\ell < Y_0 \\ \ell \text{ satisfies (136)}}} (\mathscr{Y} \setminus \mathscr{Y}_\ell) \Big| \leq$$

$$|\mathscr{Y}| - \sum_{\substack{\ell < Y_0 \\ \ell \text{ satisfies (136)}}} |\mathscr{Y}_\ell| + \sum_{\ell_1 < \ell_2 < Y_0} |\mathscr{Y}_{\ell_1 \ell_2}| - \cdots + \sum_{\ell_1 < \cdots < \ell_r < Y_0} |\mathscr{Y}_{\ell_1 \cdots \ell_r}| \tag{137}$$

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

We evaluate $|\mathscr{Y}_n|$ using Hecke characters.

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

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

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

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

If ℓ satisfies (136), the requirement $\pi_\ell\big(N(\alpha)\big) \in R_\ell$ may be expressed as

$$1 - \mathscr{X}_\ell\big(N(\alpha)\big) + \frac{1}{\ell - 1} \sum_{\mathscr{X} (\text{mod } \ell)} \overline{\mathscr{X}}(\xi_\ell) \mathscr{X}\big(N(\alpha)\big) = 1. \tag{138}$$

Thus

$$|\mathscr{Y}_n| = \sum_{N(\alpha) < Y} \Big[\frac{1}{h} \sum_{\lambda \in \widehat{\mathscr{C}}} \overline{\lambda(C)} \lambda(\alpha)\Big] \prod_{\ell | n} (138). \tag{139}$$

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

Proposition 3.8. (i) *Let $\mathscr{X}$ be a non-principal finite order Hecke character $(\mathrm{mod}\ f)$ of K. Then*

$$\Big|\sum_{N(\alpha)<x}\mathscr{X}(\alpha)\Big| < C\big(|D|N(f)\big)^{1/3}[\log|D|N(f)]^2\, x^{1/3} \tag{140}$$

(ii)

$$\sum_{N(\alpha)<x} 1 = c_1 x + O\big(|D|^{1/3}(\log|D|)^2\big)x^{1/3} \tag{141}$$

where

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

This statement follows from [L], (1), (2) p. 479; for (142), see [1], (2.5).

Analyzing (138) and (139), we have that

$$|\mathscr{Y}_n| = \frac{1}{h}\sum_{N(\alpha)\le Y}\prod_{\ell|n}\Big(1-\frac{\ell-2}{\ell-1}\mathscr{X}_\ell\big(N(\alpha)\big)\Big)+\mathrm{O}(T_n) \tag{142}$$

where T_n is a bound on sums

$$\sum_{N(\alpha)<Y}\mathscr{X}(\alpha) \text{ with } \mathscr{X}(\alpha)=\lambda(\alpha)\mathscr{X}'\big(N(\alpha)\big) \tag{143}$$

where $\lambda\in\hat{\mathscr{C}}$, $\mathscr{X}'$ is a $(\mathrm{mod}\ n_1)$-Dirichlet character with $n_1|n$ and either λ or $\mathscr{X}'$ non-principal. By (140), we have

$$T_n < C|D|\cdot nY^{1/3} < C|D|Y_0^r Y^{1/3} \tag{144}$$

so the collected contribution of T_n in (137) is at most

$$C|D|Y_0^{2r}Y^{1/3} < Y^{1/2} \tag{145}$$

imposing the condition

$$|D|Y_0^r < Y^{\frac{1}{20}}. \tag{146}$$

Analyzing further (142) using (141), we obtain

$$|\mathscr{Y}_n| = \frac{c_1}{h}\cdot Y\prod_{\substack{\ell|n\\ \mathscr{X}_D(\ell)=1}}\Big[1-\frac{\ell-2}{\ell-1}\Big(1-\frac{1}{\ell}\Big)^2\Big]\cdot\prod_{\substack{\ell|n\\ \mathscr{X}_D(\ell)=0}}\Big[1-\frac{\ell-2}{\ell-1}\Big(1-\frac{1}{\ell}\Big)\Big]\cdot\prod_{\substack{\ell|n\\ \mathscr{X}_D(\ell)=-1}}\Big[1-\frac{\ell-2}{\ell-1}\Big(1-\frac{1}{\ell^2}\Big)\Big]+\mathrm{O}(Y^{1/2}) \tag{147}$$

Substituting (147) in (137) gives

$$\frac{c_1}{h}Y \prod_{\substack{\ell<Y_0\\ \ell \text{ satisfies (136)}\\ \mathscr{X}_D(\ell)=1}}\Big(1-\frac{3}{\ell}+\frac{2}{\ell^2}\Big)\cdot \prod_{\substack{\ell<Y_0\\ \ell \text{ satisfies (136)}\\ \mathscr{X}_D(\ell)=0}}\Big(1-\frac{2}{\ell}\Big)\cdot \prod_{\substack{\ell<Y_0\\ \ell \text{ satisfies (136)}\\ \mathscr{X}_D(\ell)=-1}}\Big(1-\frac{1}{\ell}-\frac{2}{\ell^2}\Big)+$$

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

$$\ll \quad \frac{|D|^{\varepsilon}}{h}Y\frac{(\log\log X)^3}{(\log Y_0)^2}+\mathrm{O}\Big(Y\Big(\frac{3\log\log Y_0}{r}\Big)^r+Y^{1/2}Y_0^r\Big). \tag{148}$$

Taking $r=10^2\log\log Y$ and $Y_0=Y^{10^{-4}(\log\log Y)^{-1}}$, we have that (146) holds and we obtain (127). This proves Lemma 3.6. □

Theorem 3.7 may be combined with Iwaniec's result [8] on representing shifted primes by the genus of a binary quadratic form (see the Appendix for a brief 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 [8] that

$$\begin{aligned}&\#\{q+a\ll X; q \text{ prime and } q+a \text{ square free and representable by the genus of } f\}\\ &\gg \frac{X}{(\log X)^{3/2+\varepsilon}}\end{aligned} \tag{149}$$

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

Corollary 3.9. *Let f be as above with discriminant $D<0$, and assume for some $\kappa>0$*

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

with X sufficiently large. Then

$$\begin{aligned}&\#\{q+a\ll X; q \textit{ prime, such that } q+a \textit{ is representable by } f\}\\ &\gg \frac{X}{(\log X)^{3/2+\varepsilon}}.\end{aligned}$$

4. Appendix

In this section we give a flavor of the ingredients of the half-dimensional sieve, and how these ingredients extend to the version of Iwaniec's theorem which gives Corollary 3.9 in the Introduction. Let $\phi(x,y)$ be a primitive positive definite binary quadratic form of discriminant $-D$ where $D<\log X$, and let

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

where R_ϕ denotes the genus of ϕ. Then Theorem 1 of [8] gives us the following lower bounds for S_1.

Theorem 4.1. *For $a\in\mathbb{Z}$ and ϕ a primitive positive definite binary quadratic form of discriminant $-D$ where $D\leq\log X$, let $S_1(X,\phi,a)$ be as above. Then for $\varepsilon>0$ we have*

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

where the implied constant does not depend on D.

The following two lemmas are essentially Theorems 2 and 3 from [8] in the case $D < \log X$, where the integer m represented by R_ϕ is assumed to be square free and $(m,D) \leq 2$.

Lemma 4.2 (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 $\theta_p \geq 1$ for $1 \leq i \leq r$, and $\theta_2 \geq 0$. Write $m = \delta n = 2^{\varepsilon_2} n$ where m is a positive square free integer (so $0 \leq \varepsilon_2 \leq 1$) such that $(n, 2D) = 1$. Then m is represented by the genus of f iff the conditions on m in Table 1 are satisfied [5].

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

$$\mathscr{L}'_p(n) = \left\{ l \mid 0 < l < p, \left(\frac{l}{p}\right) = \left(\frac{A \cdot 2^{\varepsilon_2}}{p}\right) \right\},$$

$$\mathscr{L}''_p(n) = \left\{ l \mid 0 < l < p, \left(\frac{l}{p}\right) = \left(\frac{-A \cdot 2^{\varepsilon_2} \cdot k(-D_p)}{p}\right) \right\}$$

[5] 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	$\mathscr{K}$	τ	Conditions on n	Conditions on D	
$\theta_{p_i} \geq 1,\ p_i \neq 2$	$\frac{p_i-1}{2}$	p_i	$\left(\frac{n}{p_i}\right) = \left(\frac{A\cdot 2^{\varepsilon_2}}{p_i}\right)$	none	(1)
$p\|m,\ \ \theta_p = 0$	1	1	none	$\left(\frac{-D}{p}\right) = 1$	(2)
$\varepsilon_2 = 0,\ \theta_2 = 0$	1	1	none	$D \equiv -1\ (4)$	(3)
$\varepsilon_2 = 0,\ \theta_2 = 2$	1 or 2	4	$n \equiv A\ (4)$ or $n \equiv -AD_2\ (4)$	$D_2 \equiv -1\ (4)$ or $D_2 \equiv 1\ (4)$	(4)
$\varepsilon_2 = 0,\ \theta_2 = 3$	2	8	$n \equiv A\ (8)$ or $n \equiv A(1-2D_2)\ (8)$	none	(5)
$\varepsilon_2 = 0,\ \theta_2 = 4$	1	4	$n \equiv A\ (4)$	none	(6)
$\varepsilon_2 = 0,\ \theta_2 \geq 5$	1	8	$n \equiv A\ (8)$	none	(7)
$\varepsilon_2 = 1,\ \theta_2 = 0$	1	1	none	$D \equiv -1\ (8)$	(8)
$\varepsilon_2 = 1,\ \theta_2 = 2$	1	4	$n \equiv A\,\frac{1-D_2}{2}\ (4)$	$D_2 \equiv -1\ (4)$	(9)
$\varepsilon_2 = 1,\ \theta_2 = 3$	2	8	$n \equiv -AD_2\ (8)$ 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 $\mathscr{L}'_p$ and $\mathscr{L}''_p$ always contains $(p-1)/2$ elements. Define $\mathscr{L}_2(n)$ as follows:

$$\mathscr{L}_2(n) = \begin{cases} \{l \mid 0 < l < 4,\ l \equiv A\ (4) \text{ or } l \equiv -AD_2\ (4)\} & \text{if } \varepsilon_2 = 0,\ \theta_2 = 2 \\ \{l \mid 0 < l < 8,\ l \equiv A\ (8) \text{ or } l \equiv A(1-2D_2)\ (8)\} & \text{if } \varepsilon_2 = 0,\ \theta_2 = 3 \\ \{l \mid 0 < l < 4,\ l \equiv A\ (4)\} & \text{if } \varepsilon_2 = 0,\ \theta_2 = 4 \\ \{l \mid 0 < l < 8,\ l \equiv A\ (8)\} & \text{if } \varepsilon_2 = 0, \theta_2 \geq 5 \\ \{l \mid 0 < l < 8,\ l \equiv -AD_2\ (8) \text{ or } l \equiv A(2-D_2)\ (8)\} & \text{if } \varepsilon_2 = 1, \theta_2 = 3 \\ \{l \mid 0 < l < 4,\ l \equiv -A\,\frac{D_2-1}{2}\ (4)\} & \text{if } \varepsilon_2 = 1, \theta_2 = 2,\ D_2 \equiv -1\ (4) \\ \{0\} & \text{if } \varepsilon_2 \geq \theta_2. \end{cases}$$

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

Lemma 4.3 (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 $Q = \tau_2 \cdot \prod_{p_i \mid D_2} p_i$, and let*

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

where $k(-D)$ is the square free kernel of $-D$. Then $m = 2^{\varepsilon_2}n$ 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* $l \in \mathscr{L}_2(n)$,
- *for each* $p_i \mid D_2$ *there exists* $l \in \mathscr{L}'_{p_i}(n)$ *such that* $L \equiv l\ (p_i)$.

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

Let $\mathscr{P} = \{\text{primes } p \not| D \text{ s.t. } \left(\frac{k(-D)}{p}\right) = -1\}$, 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

$$\left| \sum_{\substack{p \leq z \\ p \in \mathscr{P}}} \frac{\log p}{\phi_E(p)} - \frac{1}{2} \log z \right| < c \tag{150}$$

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:

$$\left| \sum_{\substack{p \leq z \\ p \in \mathscr{P}}} \frac{\log p}{\phi_E(p)} - \frac{1}{2} \log z \right| \ll_\varepsilon C_1 D^\varepsilon \tag{151}$$

for any $z \geq 1$. This can be seen from the proof of Theorem 3.2.1 of [5] and the fact that

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

where the implied constant depends only on ε. As in [8], let

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

for which Iwaniec shows in [8]

Lemma 4.4 (Iwaniec)**.** *Let C_0 be as above. We have*

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

Finally, we recall the following theorem:

Lemma 4.5 (Bombieri, Vinogradov)**.** *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 $Q \cdot a$
- $M = \{m \in \mathbb{N} \mid m = \frac{p-a}{\delta}, p \leq X, p \equiv \delta L + a \ (Q\delta),\ (m, D_1) = 1\}$
- $M_d = \{m \in M \mid m \equiv 0 \ (d)\}$
- $Y = \phi(E) \cdot |M| = \operatorname{Li}(X)$
- $R_d(M) = |M_d| - \frac{Y}{\phi(dE)}$
- $y = \frac{\sqrt{X}}{Q\delta D (\log X)^U}$
- $A(M, y^{1/s}) = \#\{m \in M \text{ s.t. } m \not\equiv 0 \ (p),\ y^{1/s} > p \in \mathscr{P}\}$

By Lemma 4.3, the following is precisely what is needed to evaluate S_1:

$$\begin{aligned}\sum_{\substack{|a|<f(x,y)+a=p\le X\\(x,y)=1,f\in R_\phi}} 1 &= \sum_d \sum_{L\in\mathscr{L}} \sum_{\substack{X\ge p\equiv \delta L+a\ (Q\delta)\\ q|((p-a)/\delta)\Rightarrow q\in P\\((p-a)/\delta,2D)=1, p>|a|}} 1 \\ &= \sum_{\substack{\delta\\ 2|a\delta}} \sum_{\substack{L\in\mathscr{L}\\(\delta L+a,Q\delta)=1}} \sum_{\substack{m\in M\\ q|m\Rightarrow q\in P}} 1+\mathscr{R} \qquad (152)\end{aligned}$$

where $\mathscr{R}\le 2|D|$. It is the innermost sum in (152) 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

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

From [8] we then have

$$\left||M_d|-\frac{\mathrm{Li}X}{\phi(Q\delta d)}\right|\le 2\max_{\substack{l\\(l,Q\delta d)=1}}\left|\pi(X,Q\delta d,l)-\frac{\mathrm{Li}X}{\phi(Q\delta d)}\right| \qquad (153)$$

With the notation above, the expression in (151) combined with the $\frac{1}{2}$-dimensional sieve gives the following in our case:

Theorem 4.6.

$$\begin{aligned}A(M,y^{1/s}) &\gg_\varepsilon \sqrt{\frac{e^\gamma}{\pi}}\cdot\frac{C_0Y}{\phi(E)\sqrt{\log 3y}}\cdot\left(\int_1^s\frac{dt}{\sqrt{t(t-1)}}-\frac{(\log X)^\varepsilon}{(\log 3y)^{1/10}}\right)-\sum_{\substack{d<y\\ p|d\Rightarrow p\in\mathscr{P}}}|R_d(M)|\\ &\ge \frac{C_0\cdot\sqrt{2\frac{e^\gamma}{\pi}}}{\phi(Q\delta)}\cdot\frac{X}{(\log X)^{3/2}}\cdot\left(\int_1^s\frac{dt}{\sqrt{t(t-1)}}+(\log X)^\varepsilon\cdot o(1)\right)+\mathrm{O}(X\log^{-20}X).\end{aligned}$$

The estimation of the remainder term comes from Lemma 4.5 and (153). 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

$$A(M,y^{1/s})=\sum_{\substack{m\in M\\ q|m\Rightarrow q\in P}}1+\sum_{\substack{p_1p_2m\in M\\ q|m\Rightarrow q\in P\\ y^{1/s}\le p_1,p_2\in\mathscr{P}}}1.$$

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

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

Together with Theorem 4.6, 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 [8]. Since D_1 in our case is 1 or 2, the expression Ω_D in (4.8) of [8] becomes

$$\Omega_D = c \cdot \sum_{\substack{\delta \\ 2|D\delta}} \sum_{\substack{L\in\mathscr{L} \\ (\delta L+a, Q\delta)=1}} \frac{1}{\phi(Q\delta)} \tag{154}$$

where c is a constant not depending on D (coming from the products over $p|D_1$ in (4.8) of [8]) and $\delta = 1$ or 2 as in Table 1. Note that the innermost sum of the expression in (4.8) is $\gg_\varepsilon D^{-\varepsilon}$ for $\varepsilon > 0$. This follows from $|\mathscr{L}| = \prod_{p|D_2}(p-1)/2 \gg_{\varepsilon'} D^{1-\varepsilon'}$. Define

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

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

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

Combined with Theorem 1 of [8], this gives us the following bounds for $S_1(\phi, X, a)$ where $D \leq \log X$ and $\delta = 1$ or 2:

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

where the implied constants do not depend on D,

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

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

and $\Omega_D \gg_\varepsilon D^{-\varepsilon}$ as well for $\varepsilon > 0$. This gives us the desired generalization of Iwaniec's theorem to Theorem 4.1.

REFERENCES

[1] V. Blomer, *Binary quadratic forms with large discriminants and sums of two squareful numbers*, J. reine angew. Math. **569** (2004), 213–234

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

[3] J. Bourgain, E. Fuchs, *A proof of the positive density conjecture for integer Apollonian circle packings*, J. Amer. Math. Soc., **24** (2011), 945-967

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

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

[6] E. Golubeva, *Representation of the large numbers by binary quadratic forms*, J. Math. Sciences, **89**, No. 1 (1998), 951–954

[7] 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

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

[9] H. Iwaniec, E. Kowalski, *Analytic Number Theory*, AMS Colloquium Publications **53** (2004)

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

[11] E. Landau, *Verallgemeinerung eines Pólyaschen Satzes auf algebraische Zahlkörper*, Nachr. Kgl. Ges. Wiss. Göttingen, Math-Phys. Kl, (1918), 478–488

[12] T. Tao, V. Vu *Additive combinatorics*, Cambridge University Press, 2006

[13] M. Tarnauceanu, Bull. Math. Ser. Roum **53** (101), No 4, 2010, 373–386

INSTITUTE FOR ADVANCED STUDY, 1 EINSTEIN DRIVE, PRINCETON, NJ 08540

E-mail address: bourgain@math.ias.edu

DEPARTMENT OF MATHEMATICS, 970 EVANS HALL, UNIVERSITY OF CALIFORNIA, BERKELEY CA 94720-3840

E-mail address: efuchs@math.berkeley.edu