

## Vinogradov’s three primes theorem with primes having given primitive roots

BY C. FREI

University of Manchester, School of Mathematics, Oxford Road, Manchester M13 9PL, UK  
e-mail: [christopher.frei@manchester.ac.uk](mailto:christopher.frei@manchester.ac.uk)

P. KOYMANS

Universiteit Leiden, Mathematisch Instituut, Niels Bohrweg 1, Leiden,  
2333 CA, Netherlands.

e-mail: [p.h.koymans@math.leidenuniv.nl](mailto:p.h.koymans@math.leidenuniv.nl)

AND E. SOFOS

Max-Planck-Institut für Mathematik, Vivatsgasse 7, Bonn, 53072, Germany.  
e-mail: [sofos@mpim-bonn.mpg.de](mailto:sofos@mpim-bonn.mpg.de)

(Received 18 April 2018; revised 11 July 2019)

### Abstract

The first purpose of our paper is to show how Hooley’s celebrated method leading to his conditional proof of the Artin conjecture on primitive roots can be combined with the Hardy–Littlewood circle method. We do so by studying the number of representations of an odd integer as a sum of three primes, all of which have prescribed primitive roots. The second purpose is to analyse the singular series. In particular, using results of Lenstra, Stevenhagen and Moree, we provide a partial factorisation as an Euler product and prove that this does not extend to a complete factorisation.

2010 Mathematics Subject Classification: 11P32 (11P55, 11R45)

---

### 1. Introduction

Can we represent an odd integer as a sum of 3 odd primes all of which have 27 as a primitive root? In [10], Lenstra considered the distribution of primes with a fixed primitive root and lying in an arithmetic progression. One of his results [10, theorem (8.3)] states that if  $b \not\equiv 5 \pmod{12}$  then either there are no primes  $p \equiv b \pmod{12}$  having 27 as a primitive root or there is exactly one such prime, namely  $p = 2$ . Hence, unless  $n \equiv 3 \pmod{12}$ , no such representation exists.

In this paper, we are interested in the converse direction, at least for all sufficiently large values of  $n$ . The existence of infinitely many primes with a given primitive root  $a$  is currently not known unconditionally for any  $a \in \mathbb{Z}$ , so we need to be content with working under the assumption of a certain generalised Riemann hypothesis, sometimes called *Hooley’s Riemann Hypothesis*. For any non-zero integer  $a$ , we will write  $\text{HRH}(a)$  for the hypothesis that:

for all square-free  $k \in \mathbb{N}$ , the Dedekind zeta function of the number field  $\mathbb{Q}(\zeta_k, \sqrt[k]{a})$ , where  $\zeta_k \in \mathbb{C}$  is a primitive  $k$ th root of unity, satisfies the Riemann hypothesis.

Our main theorem can be seen as a combination of the classical conditional result of Hardy and Littlewood [4] towards ternary Goldbach with Hooley’s [7] conditional proof of Artin’s conjecture.

**THEOREM 1.1.** *Let  $\mathbf{a} = (a_1, a_2, a_3) \in \mathbb{Z}^3$  such that no  $a_i$  is  $-1$  or a square. Assuming  $\text{HRH}(a_i)$  for  $i = 1, 2, 3$ , we have*

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i: \mathbb{F}_{p_i}^* = \langle a_i \rangle}} \prod_{i=1}^3 \log p_i = \mathcal{A}_{\mathbf{a}}(n)n^2 + o(n^2), \quad \text{as } n \rightarrow +\infty,$$

with an explicit factor  $\mathcal{A}_{\mathbf{a}}(n) \in \mathbb{R}_{\geq 0}$  that satisfies  $\mathcal{A}_{\mathbf{a}}(n) \gg_{\mathbf{a}} 1$ , whenever  $\mathcal{A}_{\mathbf{a}}(n) > 0$ .

The main part of this paper is devoted to the description and investigation of the factor  $\mathcal{A}_{\mathbf{a}}(n)$ . In particular, a product decomposition of  $\mathcal{A}_{\mathbf{a}}(n)$  will allow us to interpret Theorem 1.1 as an incarnation of a local-global principle and gives the following as a simple consequence.

**COROLLARY 1.2.** *Assume  $\text{HRH}(27)$ . Let  $n$  be a sufficiently large odd integer. Then there are odd primes  $p_1, p_2, p_3$  with  $27$  as a primitive root and  $n = p_1 + p_2 + p_3$  if and only if  $n \equiv 3 \pmod{12}$ .*

We can also get an explicit saving in the error term, at the cost of having to assume a stronger generalised Riemann hypothesis. Let  $\text{HRH}'(a)$  be the hypothesis that:

for each square-free  $k > 0$  all Hecke  $L$ -functions of the number field  $\mathbb{Q}(\zeta_k, \sqrt[k]{a})$  satisfy the Riemann hypothesis.

**THEOREM 1.3.** *Let  $a_1, a_2, a_3$  be three integers none of which is  $-1$  or a perfect square. Assuming  $\text{HRH}'(a_i)$  for  $i = 1, 2, 3$ , we have for  $\beta \in (0, 1)$ ,*

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i: \mathbb{F}_{p_i}^* = \langle a_i \rangle}} \prod_{i=1}^3 \log p_i = \mathcal{A}_{\mathbf{a}}(n)n^2 + O_{\mathbf{a},\beta}(n^2(\log n)^{-\beta}),$$

where the implied constant is effective and depends at most on  $a_1, a_2, a_3$  and  $\beta$ .

Before returning to the explicit description of our factor  $\mathcal{A}_{\mathbf{a}}(n)$ , let us briefly review the relevant literature on Artin’s conjecture and the ternary Goldbach problem, and introduce some necessary notation along the way.

1.1. *Artin’s conjecture*

Fix an integer  $a \neq -1$  which is not a perfect square. An old question concerns the infinitude of the sets of primes having  $a$  as a primitive root. Artin observed that the problem can

be reformulated in the setting of algebraic number theory. Denote by  $\zeta_k$  a primitive  $k$ th root of unity and define for any positive square-free integer  $k$  the number field

$$G_{a,k} := \mathbb{Q}(a^{1/k}, \zeta_k). \tag{1.1}$$

Artin's criterion states that the prime  $p$  has  $a$  as a primitive root if and only if for every prime  $q$  the rational prime  $p$  does not split completely in  $G_{a,q}$ . This led to the formulation of the following conjecture via efforts of D. H. Artin and E. Lehmer, Cunningham and Heilbronn; see [13] for a historical overview and references. Define

$$\Delta_a := \text{Disc}(\mathbb{Q}(\sqrt{a})), \text{ the discriminant of } \mathbb{Q}(\sqrt{a}) \tag{1.2}$$

$$h_a := \max \{m \in \mathbb{N} : a \text{ is an } m\text{th power}\}, \tag{1.3}$$

$$\mathcal{A}_a := \prod_{p|h_a} \left(1 - \frac{1}{p-1}\right) \prod_{p \nmid h_a} \left(1 - \frac{1}{p(p-1)}\right)$$

and for positive integers  $q$  let

$$f_a^\ddagger(q) := \prod_{p|q, p|h_a} \frac{1}{p-2} \prod_{p|q, p \nmid h_a} \frac{1}{p^2 - p - 1}.$$

Here, and throughout our paper, the letter  $p$  is reserved for rational primes. We furthermore define

$$\mathcal{L}_a := \mathcal{A}_a \cdot (1 + \mu(2|\Delta_a|) f_a^\ddagger(|\Delta_a|)),$$

where  $\mu$  is the Möbius function. Artin's conjecture then states that

$$\lim_{x \rightarrow +\infty} \frac{\#\{p \leq x : \mathbb{F}_p^* = \langle a \rangle\}}{\#\{p \leq x\}} = \mathcal{L}_a. \tag{1.4}$$

This conjecture is of substantial difficulty: there is no value of  $a$  for which the limit is known to be positive. In fact, it is not even known whether for every integer  $a$  that is not a square or  $-1$  there exists a prime having primitive root  $a$ .

A significant step in the subject has been the, conditional under HRH( $a$ ), resolution of Artin's conjecture by Hooley [7]. His method is pivotal in the present work. Notable progress was later made by Heath-Brown [5], who building on work of Gupta and Murty [2], showed unconditionally that at least  $\gg x/(\log x)^2$  primes  $p \leq x$  have primitive root  $q, r$  or  $s$ , where  $\{q, r, s\}$  is any set of non-zero integers which is multiplicative independent and such that none of  $q, r, s, -3qr, -3qs, -3rs$  or  $qrs$  is a square. There is a rather extensive list of further results, as well as certain cryptographic applications; the reader is referred to the comprehensive survey of Moree [13]. Lenstra [10] used Hooley's method to show, conditionally on HRH( $a$ ), the existence of the natural density of primes in an arithmetic progression and with  $a$  as primitive root. An explicit formula for these densities was given later by Moree [12]. To describe Moree's result we need the following notation. Let

$$\beta_a(q) := \begin{cases} (-1)^{\frac{\Delta_a}{\gcd(q, \Delta_a)} - 1} \gcd(q, \Delta_a), & \text{if } \frac{\Delta_a}{\gcd(q, \Delta_a)} \text{ is odd,} \\ 1 & \text{otherwise,} \end{cases} \tag{1.5}$$

and observe that  $\beta_a(q)$  is a fundamental discriminant in case  $\Delta_a/\gcd(q, \Delta_a)$  is odd. For positive integers  $q$  let

$$f_a^\dagger(q) := \prod_{p|h_a, p|q} \left(1 - \frac{1}{p-1}\right)^{-1} \prod_{p \nmid h_a, p|q} \left(1 - \frac{1}{p(p-1)}\right)^{-1}.$$

*Definition 1.4.* Assume that  $a \neq -1$  is a non-square integer, let  $\Delta_a, h_a$  be as in (1.2), (1.3) and assume that  $x, q$  are integers with  $q > 0$ . We define

$$\mathcal{A}_a(x \bmod q) := \mathcal{A}_a \cdot \begin{cases} \frac{f_a^\dagger(q)}{\varphi(q)} \prod_{p|x-1, p|q} \left(1 - \frac{1}{p}\right), & \text{if } \gcd(x-1, q, h_a) = \gcd(x, q) = 1, \\ 0, & \text{otherwise,} \end{cases} \tag{1.6}$$

and

$$\delta_a(x \bmod q) := \mathcal{A}_a(x \bmod q) \left(1 + \mu\left(\frac{2|\Delta_a|}{\gcd(q, \Delta_a)}\right) \left(\frac{\beta_a(q)}{x}\right) f_a^\ddagger\left(\frac{|\Delta_a|}{\gcd(q, \Delta_a)}\right)\right),$$

where  $\varphi(\cdot)$  is the Euler totient function and  $(\cdot)$  is the Kronecker quadratic symbol.

Moree’s result [12] states that, conditionally under  $\text{HRH}(a)$ , the natural density of primes in an arithmetic progression and with  $a$  as primitive root equals  $\delta_a(x \bmod q)$ . His work will prove of central importance in our interpretation of the Artin factor for the ternary Diophantine problem under study.

1.2. Ternary Goldbach problem

The ternary Goldbach problem has been one of the most central subjects of study in analytic number theory; it asserts that every odd integer greater than 5 is the sum of 3 primes. Hardy and Littlewood [4] used the circle method to provide the first serious approach to the problem; they proved an asymptotic formula for the number of representations of  $n$  as a sum of  $k$  primes ( $k \geq 3$ ) conditionally on the veracity of the generalised Riemann hypothesis. This hypothesis was removed later by Vinogradov [17]. His result states that for every  $\beta > 0$  one has for all odd integers  $n$  that

$$\sum_{p_1+p_2+p_3=n} \prod_{i=1}^3 \log p_i = \frac{1}{2} \left(\prod_p \varrho_p(n)\right) n^2 + O_\beta(n^2(\log n)^{-\beta}),$$

where the product is over all primes, the implied constant depends at most on  $\beta$ , and

$$\varrho_p(n) := p \sum_{\substack{b_1, b_2, b_3 \in (\mathbb{Z}/p\mathbb{Z})^* \\ b_1+b_2+b_3 \equiv n \pmod{p}}} \frac{1}{(p-1)^3}. \tag{1.7}$$

This can be thought as the ratio of the probability that a random vector  $\mathbf{b} \in ((\mathbb{Z}/p\mathbb{Z})^*)^3$  satisfies  $\sum_{1 \leq i \leq 3} b_i \equiv n \pmod{p}$  to the probability that a random vector  $\mathbf{b} \in (\mathbb{Z}/p\mathbb{Z})^3$  satisfies  $\sum_{1 \leq i \leq 3} b_i \equiv n \pmod{p}$ , as made clear from

$$p = \left(\sum_{\substack{b_1, b_2, b_3 \pmod{p} \\ b_1+b_2+b_3 \equiv n \pmod{p}}} \frac{1}{p^3}\right)^{-1}. \tag{1.8}$$

It should be mentioned that Helfgott [6] recently settled the ternary Goldbach problem. Using recent developments in additive combinatorics, Shao [15] provided general conditions for an infinite subset  $\mathcal{P}$  of the primes that allow solving  $n = p_1 + p_2 + p_3$  for large odd  $n$  with each  $p_i$  in  $\mathcal{P}$ . The result most related to our work is [15, theorem 1.3]; it states that if there exists  $\delta > 0$  such that the intersection of  $\mathcal{P}$  with each invertible residue class modulo every integer  $q$  has density at least  $\delta/\varphi(q)$ , then, under suitable additional assumptions,  $n = p_1 + p_2 + p_3$  is soluble within  $\mathcal{P}$ . This does not cover our situation, since if  $h_a > 1$  then the densities  $\delta_a(1 \bmod h_a)$  vanish. Furthermore, if  $h_a = 1$  then these densities could become arbitrarily close to zero. Indeed, if  $q$  is of the form  $\prod_{p \leq T} p$  for some  $T > 2$ , then it is easy to see that

$$\delta_a(1 \bmod q)\varphi(q) \leq \prod_{p \leq T} \left(1 - \frac{1}{p}\right) \ll \frac{1}{\log \log q}.$$

It would be interesting to modify his approach in order to recover some of our results, for example a lower bound of the correct order of magnitude as the one provided by Theorem 1.1. This approach would still require  $\text{HRH}(a_i)$  and besides the focal point of our paper is the ‘Artin factor’  $\mathcal{A}_a(n)$  in Theorem 1.1. A further result related to ours is that of Kane [9]. A very special case of his work provides an asymptotic for the number of solutions of  $n = p_1 + p_2 + p_3$  when each  $p_i$  lies in a prefixed Chebotarev class of a Galois extension of  $\mathbb{Q}$ . Primes with a prescribed primitive root do admit a Chebotarev description, however the number of conditions involved is not fixed.

### 1.3. The factor $\mathcal{A}_a(n)$

Let us now describe the representation of  $\mathcal{A}_a(n)$  that is obtained directly from the proof of Theorem 1.1. Define for  $q > 0$  and square-free  $k > 0$  the number field  $F_{a,q,k} := \mathbb{Q}(\zeta_q, \zeta_k, a^{1/k})$ , so that  $G_{a,k} = F_{a,k,k}$ . Moreover, for  $b \in \mathbb{Z}$  with  $\text{gcd}(b, q) = 1$ , we let  $c_{a,q,k}(b) := 1$  if the restriction of the automorphism  $\sigma_b : \zeta_q \mapsto \zeta_q^b$  of  $\mathbb{Q}(\zeta_q)$  to  $\mathbb{Q}(\zeta_q) \cap G_{a,k}$  is the identity and we otherwise let  $c_{a,q,k}(b) := 0$ . We use the usual notation  $e_q(z) := \exp(2\pi iz/q)$ , for  $z \in \mathbb{C}, q \in \mathbb{N}$ . The exponential sum

$$S_{a,q,k}(z) := \sum_{b \in (\mathbb{Z}/q\mathbb{Z})^*} c_{a,q,k}(b)e_q(zb) \tag{1.9}$$

and the entities

$$L_{a,q,k}(z) := \prod_{i=1}^3 S_{a_i,q,k_i}(z),$$

$$d_{a,k}(q) := \prod_{i=1}^3 [F_{a_i,q,k_i} : \mathbb{Q}]$$

will play a central role throughout this paper. For positive square-free  $k_1, k_2, k_3$  we define

$$\mathfrak{S}_{a,k}(n) := \sum_{q=1}^{\infty} \frac{1}{d_{a,k}(q)} \sum_{\substack{z \in \mathbb{Z}/q\mathbb{Z} \\ \text{gcd}(z,q)=1}} e_q(-nz)L_{a,q,k}(z). \tag{1.10}$$

It will be made clear in Section 2 that this is the *singular series* for the representation problem  $n = p_1 + p_2 + p_3$  where for each  $i$  the prime  $p_i$  splits completely in  $G_{a_i,k_i}$ . The absolute

convergence of the sum over  $q$  will be verified in Lemma 3.2. With this notation in place, the leading factor in Theorem 1.1 and Theorem 1.3 is given by

$$\mathcal{A}_{\mathbf{a}}(n) = \frac{1}{2} \left( \sum_{\mathbf{k} \in \mathbb{N}^3} \mu(k_1)\mu(k_2)\mu(k_3)\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n) \right). \tag{1.11}$$

The sum over  $\mathbf{k}$  will be shown to be absolutely convergent in Lemma 3.2. It is desirable to describe the integers  $n$  for which  $\mathcal{A}_{\mathbf{a}}(n) \neq 0$ . An important remark is that if the method of Hooley works in an Artin conjecture-related problem, then it provides a leading constant which is an infinite alternating sum of Euler products that is not obviously equal to the conjectured Artin constant. Such a phenomenon is well documented and can be observed for instance in the work of Lenstra [10], who studied the density of primes in arithmetic progressions and with a prescribed primitive root, as well as the work of Serre [14], who studied the density of primes  $p$  for which the reduction of an elliptic curve over  $\mathbb{F}_p$  is cyclic. Artin constants have not been studied in the context of Diophantine problems prior to the present work, however, we will show that  $\mathcal{A}_{\mathbf{a}}(n)$  factorises partially and we shall provide an interpretation for  $\mathcal{A}_{\mathbf{a}}(n)$ . For every positive integer  $d$  we define the densities

$$\sigma_{\mathbf{a},n}(d) := d \sum_{\substack{b_1, b_2, b_3 \pmod{d} \\ b_1 + b_2 + b_3 \equiv n \pmod{d}}} \prod_{i=1}^3 \frac{\delta_{a_i}(b_i \pmod{d})}{\mathcal{L}_{a_i}}. \tag{1.12}$$

The factor  $d$  has an explanation that is identical to the explanation of the factor  $p$  in (1.7)-(1.8). Let  $[\cdot]$  denote the least common multiple,  $v_p(\cdot)$  be the  $p$ -adic valuation and define

$$\mathfrak{D}_{\mathbf{a}} := 2^{\min\{v_2(\Delta_{a_i}): 1 \leq i \leq 3\} - \max\{v_2(\Delta_{a_i}): 1 \leq i \leq 3\}} [\Delta_{a_1}, \Delta_{a_2}, \Delta_{a_3}]. \tag{1.13}$$

**THEOREM 1.5.** *The factor  $\mathcal{A}_{\mathbf{a}}(n)$  in Theorems 1.1 and 1.3 factorises as follows,*

$$\mathcal{A}_{\mathbf{a}}(n) = \frac{1}{2} \left( \prod_{i=1}^3 \mathcal{L}_{a_i} \right) \sigma_{\mathbf{a},n}(\mathfrak{D}_{\mathbf{a}}) \prod_{p \nmid \mathfrak{D}_{\mathbf{a}}} \sigma_{\mathbf{a},n}(p). \tag{1.14}$$

Furthermore, whenever  $\mathcal{A}_{\mathbf{a}}(n) > 0$ , we have

$$\mathcal{A}_{\mathbf{a}}(n) \gg \prod_{i=1}^3 \frac{\varphi(h_{a_i})}{|\Delta_{a_i}|^2 h_{a_i}}, \tag{1.15}$$

with an absolute implied constant.

For an interpretation of the right-hand side of (1.14) see Section 1.4. The proof of (1.14) (that will be provided in Section 4.1) requires adroit manoeuvring. This is because the densities  $\delta_a(b_i \pmod{d})$  in (1.12) have a complicated dependence on  $b_i$  and also do not exhibit good factorisation properties with respect to  $d$ .

Let us furthermore comment that in contrast to the usual applications of the circle method, the constant in (1.14) does not factorise as an Euler product, see Section 4.6 for a precise statement of this phenomenon. The following consequence of Theorem 1.1 and Theorem 1.5 can be seen as an instance of a local-global principle.

COROLLARY 1.6. *Let  $a_1, a_2, a_3$  be three integers none of which is  $-1$  or a perfect square, and assume  $\text{HRH}(a_i)$  for  $i = 1, 2, 3$ . For every sufficiently large odd integer  $n$ , the following statements are equivalent:*

- (1) *There are primes  $p_1, p_2, p_3$  not dividing  $6\Delta_{a_1}\Delta_{a_2}\Delta_{a_3}$  such that each  $a_i$  is a primitive root modulo  $p_i$  and  $p_1 + p_2 + p_3 = n$ ;*
- (2) *For  $d \in \{3, \mathfrak{D}_a\}$ , there are primes  $p_1, p_2, p_3$  with  $\text{gcd}(p_1 p_2 p_3, 2d) = 1$  such that  $a_i$  is a primitive root for  $p_i$  for every  $i = 1, 2, 3$  and  $p_1 + p_2 + p_3 \equiv n \pmod{d}$ .*

Though part (2) of Corollary 1.6 may not look like a purely local statement, it is one. In fact, for any  $d$  in  $\mathbb{N}$ , solubility of the congruence modulo  $d$  in primes not dividing  $2d$  with prescribed primitive roots is equivalent to the statement that  $\sigma_{a,n}(d) > 0$ . In Lemma 4.7, we shall see that  $\sigma_{a,n}(p) > 0$  whenever  $p \nmid 3\Delta_{a_1}\Delta_{a_2}\Delta_{a_3}$ . Moreover, it is clear from the definition in (1.12), that whether  $\sigma_{a,n}(d)$  is zero or not is a local condition modulo  $d$ .

#### 1.4. Interpretation of the Artin factor for the ternary Goldbach problem

Studying the constants in any counting problem of flavour similar to that of Artin’s conjecture is a non-trivial task and has been analysed rather extensively. The problems involve primes with a fixed primitive root, primes in progressions and with a fixed primitive root and primes such that the reduction of a fixed elliptic curve over the corresponding finite field is cyclic, see the work of Serre [14]. The reader that is interested in an overview of the work that has been done on these constants so far is directed at the work of Lenstra–Stevenhagen–Moree [11], as well as the survey of Moree [13].

We now focus on the interpretation of the “Artin-factor”  $\mathcal{A}_a(n)$  with the help of (1.14). First, the factor  $1/2$  is related to the density of solutions in  $\mathbb{R}$  of  $\sum_{1 \leq i \leq 3} x_i = n$  and it has the exact same interpretation as in the classical situation of ternary Goldbach, and therefore, we do not further comment on this.

The term

$$\mathcal{L}_{a_1} \mathcal{L}_{a_2} \mathcal{L}_{a_3}$$

in (1.14) should be thought of as the “probability” that for all  $i = 1, 2, 3$ , a random prime  $p_i$  has primitive root  $a_i$ , see (1.4).

The factors  $\sigma_{a,n}(d)$  for  $d \in \{\mathfrak{D}_a\} \cup \{p \text{ prime} : p \nmid \mathfrak{D}_a\}$  admit an explanation that is comparable to the analogous densities in the classical case of the ternary Goldbach problem, see (1.7). There is only one difference, namely that one has to use the weight

$$\frac{\delta_{a_i}(b_i \pmod{d})}{\mathcal{L}_{a_i}},$$

instead of  $1/(p - 1)$ . This new weight equals the conditional probability that a random prime lies in the arithmetic progression  $b_i \pmod{d}$  given that it has primitive root  $a_i$ .

It would be desirable to use algebraic considerations (for example, the approach of ‘entanglement’ of splitting fields as in the work of Lenstra–Stevenhagen–Moree [11]), to provide a prediction for  $\mathcal{A}_a(n)$  with a method that is different to the one in Section 4.1.

#### 1.5. The case where all primitive roots are equal

In our next theorem, we provide an explicit description of the local conditions in Corollary 1.6, but for space considerations we do so only in the important case where

$$a_1 = a_2 = a_3 =: a.$$

The first row of the following table contains the discriminant of  $\mathbb{Q}(\sqrt{a})$  and the second row contains the power properties of  $a$ . For example, if  $a$  is a cube, but not a fifth power, we shall write  $a \in \mathbb{Z}^3 \setminus \mathbb{Z}^5$ .

THEOREM 1.7. *Let  $a \neq -1$  be a non-square integer and  $n \in \mathbb{N}$ . Then the ‘Artin factor’*

$$\mathcal{A}_{(a,a,a)}(n)$$

*is strictly positive if and only if  $n$  satisfies the congruence conditions in the third row of the following table.*

Disc( $\mathbb{Q}(\sqrt{a})$ )	Power properties of $a$	Congruence conditions for $n$
-3	$\mathbb{Z} \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 6)
-4	$\mathbb{Z} \setminus (\{-1\} \cup \mathbb{Z}^2)$	1 (mod 4)
5	$\mathbb{Z} \setminus (\{-1\} \cup \mathbb{Z}^2)$	1 (mod 2) and not 0 (mod 5)
12	$\mathbb{Z} \setminus (\{-1\} \cup \mathbb{Z}^2 \cup \mathbb{Z}^3)$	3, 5, 7, 9 (mod 12)
12	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 12)
-15	$\mathbb{Z} \setminus (\{-1\} \cup \mathbb{Z}^2 \cup \mathbb{Z}^3 \cup \mathbb{Z}^5)$	1 (mod 2) and not 0 (mod 15)
-15	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2 \cup \mathbb{Z}^5)$	1 (mod 2) and 3, 6, 9, 12 (mod 15)
-15	$\mathbb{Z}^5 \setminus (\{-1\} \cup \mathbb{Z}^2 \cup \mathbb{Z}^3)$	1 (mod 2) and not 0, 1, 2, 7, 8, 14 (mod 15)
-15	$\mathbb{Z}^{15} \setminus (\{-1\} \cup \mathbb{Z}^2)$	12 (mod 15)
-20	$\mathbb{Z}^5 \setminus (\{-1\} \cup \mathbb{Z}^2)$	1 (mod 2) and not 1 (mod 20)
21	$\mathbb{Z}^7 \setminus (\{-1\} \cup \mathbb{Z}^2 \cup \mathbb{Z}^3)$	1 (mod 2) and not 8 (mod 21)
21	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2 \cup \mathbb{Z}^7)$	3 (mod 6)
21	$\mathbb{Z}^{21} \setminus (\{-1\} \cup \mathbb{Z}^2)$	1 (mod 2) and 3, 6, 12, 15 (mod 21)
$\pm 24$	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 6)
60	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 6)
60	$\mathbb{Z}^5 \setminus (\{-1\} \cup \mathbb{Z}^2 \cup \mathbb{Z}^3)$	1 (mod 2) and not 31, 41 (mod 60)
-84	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 6)
105	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 6)
$\pm 120$	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 6)
$\pm 168$	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 6)
-420	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 6)
$\pm 840$	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 6)
every other value	$\mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$	3 (mod 6)
every other value	$\mathbb{Z} \setminus (\{-1\} \cup \mathbb{Z}^2 \cup \mathbb{Z}^3)$	1 (mod 2)

The last two rows refer to any value of Disc( $\mathbb{Q}(\sqrt{a})$ ) not considered in an earlier row.

Theorem 1.7 enables one to describe all large enough integers having a representation as a sum of 3 primes with a prescribed primitive root. One such example is Corollary 1.2, whose proof we give now.

*Proof of Corollary 1.2* If  $n$  is a sum of 3 odd primes all of which have primitive root 27, we saw in the first paragraph of our paper that  $n$  must be 3 (mod 12). For the opposite direction we observe that if  $a = 27$  then we have Disc( $\mathbb{Q}(\sqrt{a})$ ) = 12 and  $a \in \mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$ , hence consulting the fifth row in the table of Theorem 1.7 we see that, conditionally on HRH(27),



every sufficiently large integer  $n \equiv 3 \pmod{12}$  is a sum of three odd primes with primitive root 27.

1.6. Structure of the paper

We study a generalisation of the ternary Goldbach problem in Section 2, where each of the three primes involved satisfies certain splitting conditions in a different number field extension of  $\mathbb{Q}$ . The main result of Section 2 is Proposition 2.1, whose proof is given in Section 2.3.

Next, Section 3.1 contains the first steps for the combination of Hooley's argument [7] and the Hardy–Littlewood circle method. Theorem 1.1 will be proved in Section 3.2, while Theorem 1.3 is verified in Section 3.3.

The rest of our paper, namely Section 4, deals with the 'Artin factor'  $\mathcal{A}_a(n)$ . The former part of Theorem 1.1, viz. (1.14), is verified in Section 4.1, while the latter part, viz. (1.15), is established in Section 4.2. Corollary 1.6 and Theorem 1.7 are proved in Section 4.4 and Section 4.5 respectively. Finally, we show that  $\mathcal{A}_a(n)$  does not factorise as an Euler product in Section 4.6.

*Notation.* The letters  $p$  and  $\ell$  will always denote a rational prime. The entities  $a_i, h_{a_i}, \Delta_{a_i}$  are considered constant throughout our work, thus the dependence of implied constants on them will not be recorded. On several occasions our implied constants are absolute, this will always be specified. Finally, we will use the notation

$$e(z) := \exp(2\pi iz) \text{ and } e_q(z) := \exp(2\pi iz/q), \quad (z \in \mathbb{C}, q \in \mathbb{N}).$$

2. Uniform ternary Goldbach with certain splitting conditions

In this section the letters  $k, k_i$  shall refer exclusively to positive square-free integers. Recall (1.1) and define

$$\text{Spl}(G_{a,k}) := \{p \text{ prime in } \mathbb{N} : p \text{ splits completely in } G_{a,k}\}. \tag{2.1}$$

We study the asymptotics of the representation function

$$V_{\mathbf{a},\mathbf{k}}(n) := \sum_{\substack{p_1+p_2+p_3=n \\ \forall i: p_i \in \text{Spl}(G_{a_i,k_i})}} \prod_{i=1}^3 \log p_i. \tag{2.2}$$

We will see that the singular series related to the estimation of  $V_{\mathbf{a},\mathbf{k}}(n)$  is the series  $\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)$  introduced in (1.10). Kane [9] studied a very general set of problems, one case of which is that of evaluating  $V_{\mathbf{a},\mathbf{k}}(n)$  asymptotically. His work provides a function  $f_{\mathbf{a}}$  such that for each  $B > 0$  and square-free  $k_1, k_2, k_3$  we have

$$V_{\mathbf{a},\mathbf{k}}(n) = \frac{1}{2} \mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)n^2 + O_B\left(|f_{\mathbf{a}}(\mathbf{k})| \frac{n^2}{(\log n)^B}\right), \tag{2.3}$$

where the implied constant depends at most on  $\mathbf{a}$  and  $B$ . This can be deduced by taking

$$N := n, \quad X := n, \quad k := 3, \quad a_i := 1, \quad K_i := G_{a_i,k_i} \text{ and } C_i := \text{id}_{G_{a_i,k_i}}$$

in [9, theorem 2]. With this choice the constant  $C_\infty$  in [9, theorem 2] equals  $n^2/2$  and a long but straightforward computation allows one to show that the 'singular series'  $\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)$

can be factored into the remaining parts of the main term in the asymptotic formula [9, equation (1.2)].

Our aim in this section is to prove the following result, conditional on the hypothesis  $\text{HRH}'(a_i)$  introduced before Theorem 1.3. It constitutes a version of (2.3) that has a power saving in the error term and an explicit and polynomial dependence on the  $k_i$ . As is surely familiar to circle method experts, an error term of this quality is currently out of reach unconditionally even in the setting of the classical ternary Goldbach problem.

**PROPOSITION 2.1.** *Assume  $\text{HRH}'(a_i)$  for  $i = 1, 2, 3$ . The following estimate holds for all square-free  $k_1, k_2, k_3$  with  $1 \leq k_1, k_2, k_3 \leq n$  and with an implied constant depending at most on  $\mathbf{a}$ ,*

$$V_{\mathbf{a},k}(n) = \frac{1}{2} \mathfrak{S}_{\mathbf{a},k}(n)n^2 + O\left(n^{11/6}(\log n)^6 \left(\max_{1 \leq i \leq 3} k_i\right)^6\right).$$

2.1. Algebraic considerations

We shall need explicit bounds for certain algebraic quantities associated to  $G_{a,k}$ . This subsection is mostly devoted to providing the necessary estimates.

Recall the definitions of  $\Delta_a$  and  $h_a$ , given in (1.2) and (1.3). We begin by determining the degree of the number field  $F_{a,q,k}$  defined at the start of Section 1.3 (see [12, lemma 2.3]).

**LEMMA 2.2.** *For  $k$  square-free let  $k' = k / \gcd(k, h_a)$ . Then  $[F_{a,q,k} : \mathbb{Q}] = k' \varphi([q, k]) / \varepsilon(q, k)$ , where*

$$\varepsilon(q, k) = \begin{cases} 2, & \text{if } 2 \mid k \text{ and } \Delta_a \mid [q, k], \\ 1, & \text{otherwise.} \end{cases}$$

**LEMMA 2.3.** *Let  $k' = k / \gcd(k, h_a)$  and  $a = g_1^{\gcd(k, h_a)} g_2^k$ , with  $g_1$  free of  $k'$ th powers. Then*

$$\frac{\log |\text{Disc}(F_{a,q,k})|}{[F_{a,q,k} : \mathbb{Q}]} \leq \log k' + \log([q, k]) + 2 \log |g_1|.$$

*Proof.* We have  $|\text{Disc}(F_{a,q,k})| = \mathfrak{N}(\Delta_{F_{a,q,k}/\mathbb{Q}(\zeta_{[q,k]})}) |\text{Disc}(\mathbb{Q}(\zeta_{[q,k]}))|^{[F_{a,q,k}:\mathbb{Q}(\zeta_{[q,k]})]}$ , where  $\mathfrak{N}$  is the absolute norm of an ideal and  $\Delta_{F_{a,q,k}/\mathbb{Q}(\zeta_{[q,k]})}$  is the relative discriminant ideal. Any  $k'$ -th root  $\alpha \in F_{a,q,k}$  of  $g_1$  generates  $F_{a,q,k}$  over  $\mathbb{Q}(\zeta_{[q,k]})$ , so its different  $d(\alpha) \neq 0$  is in the different ideal of  $F_{a,q,k}/\mathbb{Q}(\zeta_{[q,k]})$ . Since the minimal polynomial of  $\alpha$  over  $\mathbb{Q}(\zeta_{[q,k]})$  divides  $x^{k'} - g_1$ , we find that  $k' \alpha^{k'-1}$  is a multiple of  $d(\alpha)$  in  $\mathcal{O}_{F_{a,q,k}}$ , and thus in the different ideal as well. Hence,

$$\mathfrak{N}(\Delta_{F_{a,q,k}/\mathbb{Q}(\zeta_{[q,k]})}) \leq |N_{F_{a,q,k}/\mathbb{Q}}(k' \alpha^{k'-1})| \leq (k')^{[F_{a,q,k}:\mathbb{Q}]} |g_1|^{(k'-1)\varphi([q,k])} \leq (k')^{[F_{a,q,k}:\mathbb{Q}]} |g_1|^{2[F_{a,q,k}:\mathbb{Q}]}.$$

To complete the proof, use  $|\text{Disc}(\mathbb{Q}(\zeta_{[q,k]}))| = [q, k]^{\varphi([q,k])} \prod_{p|qk} p^{-\varphi([q,k])/(p-1)} \leq [q, k]^{\varphi([q,k])}$ .

Clearly, the intersection  $\mathbb{Q}(\zeta_q) \cap G_{a,k}$  contains  $\mathbb{Q}(\zeta_{\gcd(q,k)})$ . More precisely, it is determined as follows (see [12, lemma 2.4]).

LEMMA 2.4. *We have*

$$[\mathbb{Q}(\zeta_q) \cap G_{a,k} : \mathbb{Q}(\zeta_{\gcd(q,k)})] = \begin{cases} 2 & \text{if } 2 \mid k, \Delta_a \nmid k \text{ and } \Delta_a \mid [q, k] \\ 1 & \text{otherwise.} \end{cases}$$

In the first case, the integer  $\beta_a(q)$  defined in (1.5) is a fundamental discriminant and we have  $\mathbb{Q}(\zeta_q) \cap G_{a,k} = \mathbb{Q}(\zeta_{\gcd(q,k)}, \sqrt{\beta_a(q)})$ .

Since both  $\mathbb{Q}(\zeta_q)$  and  $G_{a,k}$  are normal, the same holds for their compositum  $F_{a,q,k}$ . We investigate the existence of certain elements of the Galois group  $\text{Gal}(F_{a,q,k}/\mathbb{Q})$ . Recall the definitions of  $\sigma_b$  and  $c_{a,q,k}(b)$  from the start of Section 1.3.

LEMMA 2.5. *Let  $b \in \mathbb{Z}$  with  $\gcd(b, q) = 1$ . The following are equivalent:*

(1) *there is an automorphism  $\sigma \in \text{Gal}(F_{a,q,k}/\mathbb{Q})$  with*

$$\sigma|_{\mathbb{Q}(\zeta_q)} = \sigma_b \text{ and } \sigma|_{G_{a,k}} = \text{id}_{G_{a,k}}; \tag{2.4}$$

(2)  $c_{a,q,k}(b) = 1$ ;

(3) *with  $\beta_a(q)$  defined in (1.5), we have*

$$b \equiv 1 \pmod{\gcd(q, k)}, \quad \text{and} \tag{2.5}$$

$$2 \mid k, \Delta_a \nmid k, \Delta_a \mid [q, k] \text{ implies that } \left(\frac{\beta_a(q)}{b}\right) = 1. \tag{2.6}$$

Moreover, if  $\sigma$  as in (1) exists, it is unique and in the center of  $\text{Gal}(F_{a,q,k}/\mathbb{Q})$ .

*Proof.* Write  $I := \mathbb{Q}(\zeta_q) \cap G_{a,k}$ . The map  $\sigma \mapsto (\sigma|_{\mathbb{Q}(\zeta_q)}, \sigma|_{G_{a,k}})$  provides an isomorphism

$$\text{Gal}(F_{a,q,k}/\mathbb{Q}) \cong \{(\sigma_1, \sigma_2) \in \text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \times \text{Gal}(G_{a,k}/\mathbb{Q}) : \sigma_1|_I = \sigma_2|_I\}.$$

Thus, an automorphism  $\sigma$  with (2.4) exists if and only if  $c_{a,q,k}(b) = 1$ , proving the equivalence of (1) and (2). In this case  $\sigma$  is necessarily unique and clearly in the center of  $\text{Gal}(F_{a,q,k}/\mathbb{Q})$ , because the Galois group  $\text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$  is abelian and  $\text{id}_{G_{a,k}}$  is in the center of  $\text{Gal}(G_{a,k}/\mathbb{Q})$ . Thus, let us study the conditions under which  $c_{a,q,k}(b) = 1$ .

Since  $\mathbb{Q}(\zeta_{\gcd(q,k)}) \subset I$  and  $\sigma_b|_{\mathbb{Q}(\zeta_{\gcd(q,k)})}$  coincides with the automorphism  $\zeta \mapsto \zeta^{b \pmod{\gcd(q,k)}}$ , the condition (2.5) is clearly necessary. Thus, we assume it to hold from now on, whence  $\sigma_b|_{\mathbb{Q}(\zeta_{\gcd(q,k)})} = \text{id}_{G_{a,k}}$ . If any of the assumptions in (2.6) do not hold, then we have  $I = \mathbb{Q}(\zeta_{\gcd(q,k)})$  by Lemma 2.4, and thus  $c_{a,q,k}(b) = 1$ . If all of the assumptions in (2.6) hold, then, invoking Lemma 2.4 once more, we find that  $\sqrt{\beta_a(q)} \in \mathbb{Q}(\zeta_q)$  and  $c_{a,q,k}(b) = 1$  is equivalent to

$$\sigma_b(\sqrt{\beta_a(q)}) = \sqrt{\beta_a(q)}. \tag{2.7}$$

Since  $\beta_a(q)$  is a fundamental discriminant, we may invoke [12, lemma 2.2] to see that (2.7) is equivalent to  $(\beta_a(q)/b) = 1$ .

### 2.2. Consequences of HRH’(a)

In this section we use the hypothesis HRH’(a) to provide estimates for certain exponential sums related to the estimation of  $V_{a,k}(n)$ .

LEMMA 2.6. Assume HRH' (a). For any square-free  $k$  and coprime integers  $c, q$  we have

$$\sum_{\substack{p \leq x \\ p \in \text{Spl}(G_{a,k})}} (\log p) e_q(cp) = \frac{x}{\varphi(q)[G_{a,k} : \mathbb{Q}]} \sum_{\substack{\chi \pmod{q} \\ \chi \circ \mathfrak{N} = \chi_0}} \overline{\chi(c)} \tau(\chi) + O(k^2 \sqrt{qx} (\log qx)^2).$$

Here,  $\chi$  runs through all Dirichlet characters modulo  $q$  for which  $\chi \circ \mathfrak{N}$ , considered as a ray class character modulo  $q \mathcal{O}_{G_{a,k}}$ , is the trivial ray class character  $\chi_0$ . Moreover,  $\tau(\chi)$  denotes the Gauss sum  $\tau(\chi) = \sum_{y \pmod{q}} \chi(y) e_q(y)$ .

*Proof.* We have

$$\sum_{\substack{p \leq x \\ p \in \text{Spl}(G_{a,k})}} (\log p) e_q(cp) = \sum_{\substack{p \leq x, p \nmid q \\ p \in \text{Spl}(G_{a,k})}} (\log p) e_q(cp) + O((\log q)^2). \tag{2.8}$$

Bringing into play the Dirichlet characters modulo  $q$  allows us to insert, for  $p \nmid q$ ,

$$e_q(cp) = \frac{1}{\varphi(q)} \sum_{b \pmod{q}} \sum_{\chi \pmod{q}} \chi(b) \overline{\chi(cp)} e_q(b) = \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \overline{\chi(cp)} \tau(\chi)$$

into (2.8), thus showing the validity of

$$\sum_{\substack{p \leq x \\ p \in \text{Spl}(G_{a,k})}} (\log p) e_q(cp) = \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \overline{\chi(c)} \tau(\chi) \psi_{a,k}(x, \overline{\chi}) + O((\log q)^2),$$

where

$$\begin{aligned} \psi_{a,k}(x, \chi) &:= \sum_{\substack{p \leq x \\ p \in \text{Spl}(G_{a,k})}} (\log p) \chi(p) = \frac{1}{[G_{a,k} : \mathbb{Q}]} \sum_{\substack{\mathfrak{N} \mathfrak{p} \leq x \\ \deg(\mathfrak{p})=1}} (\log \mathfrak{N} \mathfrak{p}) \chi(\mathfrak{N} \mathfrak{p}) \\ &= \frac{1}{[G_{a,k} : \mathbb{Q}]} \sum_{\mathfrak{N} \mathfrak{n} \leq x} \Lambda(\mathfrak{n}) \chi(\mathfrak{N} \mathfrak{n}) + O(\sqrt{x} \log x). \end{aligned}$$

Here and for the rest of this section  $\mathfrak{p}$  denotes a prime ideal in  $\mathcal{O}_{G_{a,k}}$ ,  $\deg(\mathfrak{p})$  denotes its inertia degree over  $\mathbb{Q}$ ,  $\mathfrak{n}$  denotes an ideal in  $\mathcal{O}_{G_{a,k}}$ , and  $\Lambda$  is the von Mangoldt function on ideals of  $\mathcal{O}_{G_{a,k}}$ , defined by  $\Lambda(\mathfrak{p}^e) := \log \mathfrak{N} \mathfrak{p}$  for  $e \geq 1$  and  $\Lambda(\mathfrak{n}) := 0$  in all other cases. Observing that  $\chi \circ \mathfrak{N}$  defines a character of the ray class group of  $G_{a,k}$  modulo  $q \mathcal{O}_{G_{a,k}}$ , we can consider its Hecke  $L$ -function,

$$L(s, \chi) := \sum_{\mathfrak{n} \neq 0} \chi(\mathfrak{N} \mathfrak{n}) (\mathfrak{N} \mathfrak{n})^{-s}.$$

It is now easy to see that  $-L'(s, \chi)/L(s, \chi) = \sum_{\mathfrak{n} \neq 0} \Lambda(\mathfrak{n}) \chi(\mathfrak{N} \mathfrak{n}) (\mathfrak{N} \mathfrak{n})^{-s}$ . The Ramanujan–Pettersson conjecture is obviously true for  $L(s, \chi)$ , since it is true for any Hecke  $L$ -function. Hence [8, theorem 5.15] implies that

$$\sum_{\mathfrak{N} \mathfrak{n} \leq x} \Lambda(\mathfrak{n}) \chi(\mathfrak{N} \mathfrak{n}) = r_\chi x + O(x^{\frac{1}{2}} (\log x) \log(x^{[G_{a,k} : \mathbb{Q}]} q(\chi))),$$

where  $r_\chi$  is the order of the pole of  $L(s, \chi)$  at  $s=1$ . For the definition of  $q(\chi)$ , see [8, page 95]. Furthermore, on [8, page 129] it is proven that  $q(\chi) \leq$

$4^{[G_{a,k}:\mathbb{Q}]}\text{Disc}(G_{a,k})|q|^{[G_{a,k}:\mathbb{Q}]}$ . Our next task is to make explicit the value of  $r_\chi$ . If  $\chi \circ \mathfrak{N}$  is the trivial ray class character  $\chi_0$  modulo  $\mathcal{O}_{G_{a,k}}$ , then we have  $r_\chi = 1$ ; otherwise we have  $r_\chi = 0$ . Using  $|\tau(\chi)| \leq \sqrt{q}$  and Lemma 2.3 we can substitute in (2.2) to find that

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \overline{\chi(c)} \tau(\chi) \psi_{a,k}(x, \overline{\chi}) = \frac{x\varphi(q)^{-1}}{[G_{a,k}:\mathbb{Q}]} \sum_{\substack{\chi \pmod{q} \\ \chi \circ \mathfrak{N} = \chi_0}} \overline{\chi(c)} \tau(\chi) + O([G_{a,k}:\mathbb{Q}]\sqrt{qx}(\log qx)^2),$$

thus concluding our proof upon observing that  $[G_{a,k}:\mathbb{Q}] = [F_{a,k,k}:\mathbb{Q}] \leq k^2$ .

Although it is possible to directly evaluate the main term in Lemma 2.6, we will instead use the following trick.

LEMMA 2.7. *Under the same conditions as in Lemma 2.6 we have*

$$\sum_{\substack{p \leq x \\ p \in \text{Spl}(G_{a,k})}} (\log p) e_q(cp) = \frac{S_{a,q,k}(c)}{[F_{a,q,k}:\mathbb{Q}]} x + o_{q,k}(x), \text{ as } x \rightarrow +\infty.$$

*Proof.* Partitioning in progressions modulo  $q$  we see that, owing to (2.8), the sum over  $p$  in our lemma is equal to the following quantity up to an error of size  $o_{q,k}(x)$ ,

$$\sum_{b \in (\mathbb{Z}/q\mathbb{Z})^*} e_q(bc) \sum_{\substack{p \leq x \\ p \equiv b \pmod{q} \\ p \in \text{Spl}(G_{a,k})}} \log p.$$

By Lemma 2.5 there exists an automorphism  $\sigma$  of  $F_{a,q,k}$  satisfying

$$\sigma|_{\mathbb{Q}(\zeta_q)} = \sigma_b \text{ and } \sigma|_{G_{a,k}} = \text{id}_{G_{a,k}}$$

if and only if  $c_{a,q,k}(b) = 1$ . Furthermore, if such an automorphism exists, it is unique. The lemma is now a consequence of Chebotarev's density theorem.

Combining Lemma 2.6 and Lemma 2.7 proves the following lemma.

LEMMA 2.8. *Under the same assumptions as in Lemma 2.6 we have*

$$\sum_{\substack{p \leq x \\ p \in \text{Spl}(G_{a,k})}} (\log p) e_q(cp) = \frac{S_{a,q,k}(c)x}{[F_{a,q,k}:\mathbb{Q}]} + O(k^2 \sqrt{qx} \log^2 qx).$$

Define for a square-free integer  $k > 0$  the exponential sum

$$f_{a,k}(\alpha) = \sum_{\substack{p \leq n \\ p \in \text{Spl}(G_{a,k})}} (\log p) e(\alpha p), \quad (\alpha \in \mathbb{R}). \tag{2.9}$$

The next lemma is easily proved via partial summation and Lemma 2.8.

LEMMA 2.9. *Assume HRH'(a). Let k be square-free integer and define  $\alpha = c/q + \beta$ , where  $(c, q) = 1$ . Then*

$$f_{a,k}(\alpha) = \frac{S_{a,q,k}(c)}{[F_{a,q,k}:\mathbb{Q}]} \int_0^n e(\beta x) dx + O(k^2(1 + |\beta|n)\sqrt{qn}(\log qn)^2).$$

It will be necessary to gain a better understanding of the exponential sums  $S_{a,q,k}(c)$ . We start by studying  $c_{a,q,k}(\cdot)$  in the next lemma, whose proof follows directly from (2.5) and (2.6).

LEMMA 2.10. *Let  $b, q$  be coprime integers and factor  $q$  as  $q = d \prod_{i=1}^l p_i^{e_i}$  with  $d$  an integer composed of primes dividing  $\Delta_a$  and  $p_i$  distinct prime numbers not dividing  $\Delta_a$ . Then we have for any square-free integer  $k$ ,*

$$c_{a,q,k}(b) = c_{a,d,k}(b) \prod_{i=1}^l c_{a,p_i^{e_i},k}(b).$$

LEMMA 2.11. *Let  $k$  be square-free, assume that  $b, q$  are coprime integers and suppose that  $q = q_1q_2, b = b_1q_2 + b_2q_1$ , with  $q_1, q_2$  coprime. If  $\gcd(q_1, \Delta_a) = 1$  or  $\gcd(q_2, \Delta_a) = 1$ , then*

$$S_{a,q,k}(b) = S_{a,q_1,k}(b_1)S_{a,q_2,k}(b_2).$$

*Proof.* By the Chinese remainder theorem we can write each element  $y \in \mathbb{Z}/q\mathbb{Z}$  as  $y_1q_2 + y_2q_1$ , where  $y_i \in \mathbb{Z}/q_i\mathbb{Z}$ , thus showing that  $e_q(by) = e_{q_1}(b_1y_1q_2)e_{q_2}(b_2y_2q_1)$ . This leads to

$$\begin{aligned} S_{a,q,k}(b) &= \sum_{y \in (\mathbb{Z}/q\mathbb{Z})^*} c_{a,q,k}(y)e_q(by) \\ &= \sum_{y_1 \in (\mathbb{Z}/q_1\mathbb{Z})^*} e_{q_1}(b_1y_1q_2) \sum_{y_2 \in (\mathbb{Z}/q_2\mathbb{Z})^*} e_{q_2}(b_2y_2q_1)c_{a,q,k}(y_1q_2 + y_2q_1). \end{aligned}$$

By Lemma 2.10 we have  $c_{a,q,k}(y_1q_2 + y_2q_1) = c_{a,q_1,k}(y_1q_2 + y_2q_1)c_{a,q_2,k}(y_1q_2 + y_2q_1)$ . The entity  $c_{a,q,k}(y)$  is periodic (mod  $q$ ) as a function of  $y$ , thus we can write  $S_{a,q,k}(b)$  as

$$\sum_{y_1 \in (\mathbb{Z}/q_1\mathbb{Z})^*} e_{q_1}(b_1y_1q_2)c_{a,q_1,k}(y_1q_2) \sum_{y_2 \in (\mathbb{Z}/q_2\mathbb{Z})^*} e_{q_2}(b_2y_2q_1)c_{a,q_2,k}(y_2q_1)$$

and a simple linear change of variables in each sum completes the proof.

LEMMA 2.12. *For  $k$  square-free,  $b$  an integer and  $p$  a prime with  $p \nmid b\Delta_a$  we have*

$$|S_{a,p^j,k}(b)| = \begin{cases} 1, & j = 1 \\ 0, & j > 1. \end{cases}$$

*Proof.* Let us observe that (2.6) always holds for  $q = p^j$  as in the lemma, as the hypothesis is never satisfied. We first handle the case  $j = 1$ . If  $p \nmid k$  then by Lemma 2.5,  $S_{a,p,k}(b)$  is the classical Ramanujan sum and the result follows, while in the remaining case,  $p \mid k$ , the result is also immediate from (2.5). Now suppose  $j > 1$ . Again, if  $p \nmid k$ , the sum in the lemma is a Ramanujan sum and the result follows. We are therefore free to assume that  $p \mid k$ . Writing  $y = 1 + px$  we see that

$$S_{a,p^j,k}(b) = \sum_{\substack{y \pmod{p^j} \\ y \equiv 1 \pmod{p}}} e_{p^j}(by) = e_{p^j}(b) \sum_{x \pmod{p^{j-1}}} e_{p^{j-1}}(bx),$$

which is clearly sufficient since the inner sum vanishes.

LEMMA 2.13. Let  $r, Q, c \in \mathbb{Z}$  be such that  $rQ \neq 0$ ,  $\gcd(c, Q) = 1$ ,  $r$  divides  $Q$  and assume that a function  $f : \mathbb{Z} \rightarrow \mathbb{C}$  has period  $|r|$ . If we have  $|r| < |Q|$  then the following sum vanishes,

$$\sum_{b \pmod{|Q|}} e_{|Q|}(bc) f(b).$$

*Proof.* The claim becomes clear upon writing the sum in our lemma as

$$\sum_{b_0 \pmod{|r|}} e_{|Q|}(b_0 c) f(b_0) \sum_{x \pmod{|Q/r|}} e_{|Q/r|}(xc)$$

and observing that if  $|Q/r| \neq 1$ , then each exponential sum over  $x$  vanishes.

LEMMA 2.14. Let  $k$  be a square-free integer, suppose that  $q$  is composed of primes dividing  $\Delta_a$  and let  $b$  be an integer with  $\gcd(b, q) = 1$ . If  $q \nmid \Delta_a$ , then  $S_{a,q,k}(b) = 0$ .

*Proof.* First suppose  $2 \nmid k$  or  $\Delta_a \mid k$  or  $\Delta_a \nmid [q, k]$  and write  $q = p_1^{e_1} \cdots p_l^{e_l}$ . We have

$$S_{a,q,k}(b) = \prod_{i=1}^l c_{a,p_i^{e_i},k}(b),$$

therefore  $S_{a,q,k}(b) = 0$  can now be easily proved as before, as our hypotheses imply that  $e_j > 1$  for at least one  $j$ .

Now suppose that  $2 \mid k$  and  $\Delta_a \nmid k$  and  $\Delta_a \mid [q, k]$ . For  $y \in \mathbb{Z}$ , let  $f(y) := 1$  if  $y \equiv 1 \pmod{\gcd(k, q)}$  and  $(\beta_a(q)/y) = 1$ , and  $f(y) := 0$  otherwise. By Lemma 2.5 we have

$$S_{a,q,k}(b) = \sum_{y \pmod{q}} f(y) e_q(by).$$

Since  $\gcd(k, q) \mid \gcd(\Delta_a, q) = |\beta_a(q)|$  and  $\beta_a(q)$  is a fundamental discriminant, we see that  $f$  has period  $\gcd(\Delta_a, q)$ , strictly dividing  $q$  by our hypotheses. Now apply Lemma 2.13.

Combining Lemmas 2.11, 2.12 and 2.14 allows us to conclude that

$$S_{a,q,k}(b) \ll 1, \tag{2.10}$$

where the implied constant depends at most on  $a$ .

### 2.3. Proof of Proposition 2.1

Recall (2.9). Our starting point is the circle method identity,

$$\sum_{\substack{p_1+p_2+p_3=n \\ p_i \in \text{Spl}(G_{a_i,k_i})}} \prod_{i=1}^3 (\log p_i) = \int_0^1 f_{a_1,k_1}(\alpha) f_{a_2,k_2}(\alpha) f_{a_3,k_3}(\alpha) e(-n\alpha) d\alpha. \tag{2.11}$$

COROLLARY 2.15. Assume  $\text{HRH}'(a)$ , and suppose  $\alpha, c, q$  fulfil  $|\alpha - c/q| \leq q^{-1}n^{-2/3}$ ,  $\gcd(c, q) = 1$ ,  $q \leq n^{2/3}$  and that  $k$  is square-free. Then we have  $f_{a,k}(\alpha) \ll (n/q + k^2 n^{5/6})(\log n)^2$ .

*Proof.* Observe that Lemma 2.2 gives  $[F_{a,q,k} : \mathbb{Q}]^{-1} \ll \varphi([q, k])^{-1} \ll \varphi(q)^{-1} \ll (\log q)q^{-1}$ , hence, by Lemma 2.9 and (2.10) one obtains  $f_{a,k}(\alpha) \ll n(\log n)q^{-1} + k^2(1 + n^{1/3}q^{-1})\sqrt{qn}(\log n)^2$ . Our proof can then be concluded by using  $q \leq n^{2/3}$ .

Define  $P := n^\nu$ , for an absolute constant  $\nu \in (0, 1/6]$  that will be chosen later. In our situation the major arc  $\mathfrak{M}(c, q)$  is defined for coprime  $c, q$  via

$$\mathfrak{M}(q, c) := \{\alpha : |\alpha - c/q| \leq q^{-1}n^{-2/3}\},$$

while we let  $\mathfrak{M}$  be the union of all  $\mathfrak{M}(q, c)$  with  $1 \leq q \leq P, 1 \leq c \leq q, \gcd(c, q) = 1$  and define the minor arcs through  $\mathfrak{m} := [0, 1] \setminus \mathfrak{M}$ . We note here that the major arcs are pairwise disjoint. This follows from the inequality  $(qq')^{-1} > (qn^{2/3})^{-1} + (q'n^{2/3})^{-1}$ , holding for all  $n > 8$ , as  $q, q' \leq n^{1/3}$ .

COROLLARY 2.16. *Assume HRH'(a<sub>i</sub>) for 1 ≤ i ≤ 3. Then*

$$\int_{\mathfrak{m}} |f_{a_1,k_1}(\alpha) f_{a_2,k_2}(\alpha) f_{a_3,k_3}(\alpha)| d\alpha \ll n^{2-\nu} (\log n)^3 \min_i k_i^2.$$

*Proof.* By Dirichlet’s approximation theorem, for each  $\alpha$  there exist coprime integers  $c, q$  with  $|\alpha - c/q| \leq q^{-1}n^{-2/3}$  and  $1 \leq q \leq n^{2/3}$ . If  $\alpha \in \mathfrak{m}$  then  $q > n^\nu$ , hence Corollary 2.15 yields the estimate  $f_{a,k}(\alpha) \ll k^2 n^{1-\nu} (\log n)^2$ . We may assume  $k_1 \leq k_2, k_3$  with no loss of generality, therefore the integral in our lemma is  $\ll k_1^2 n^{1-\nu} (\log n)^2 \int_0^1 |f_{a_2,k_2}(\alpha) f_{a_3,k_3}(\alpha)| d\alpha$ , thus Cauchy’s inequality yields the following bound for the latter integral,

$$\ll \left( \int_0^1 |f_{a_2,k_2}(\alpha)|^2 d\alpha \right)^{1/2} \left( \int_0^1 |f_{a_3,k_3}(\alpha)|^2 d\alpha \right)^{1/2}.$$

Both integrals are at most  $\sum_{p \leq n} (\log p)^2 \ll n \log n$ , which provides the desired result.

Note that if  $\beta + c/q \in \mathfrak{M}(q, c)$  for some  $q \leq n^{1/3}$ , then Lemma 2.9 shows that

$$f_{a_i,k_i}(\alpha) = \frac{S_{a_i,q,k_i}(c)}{[F_{a_i,q,k_i} : \mathbb{Q}]} \int_0^n e(\beta x) dx + O\left(\frac{n^{5/6}}{q^{1/2}} (\log n)^2 \max_i k_i^2\right).$$

Hence the estimates

$$\int_0^n e(\beta x) dx \ll \min\{n, |\beta|^{-1}\} \quad \text{and} \quad \frac{S_{a,q,k}(c)}{[F_{a,q,k} : \mathbb{Q}]} \ll \varphi(q)^{-1}$$

show that  $f_{a_1,k_1}(c/q + \beta) f_{a_2,k_2}(c/q + \beta) f_{a_3,k_3}(c/q + \beta) - L_{a,q,k}(c) d_{a,k}(q)^{-1} \left(\int_0^n e(\beta x) dx\right)^3$  is

$$\ll \frac{\min\{n^2, |\beta|^{-2}\} n^{5/6}}{\varphi(q)^2} \frac{n^{5/6}}{q^{1/2}} (\log n)^2 \max_i k_i^2 + \frac{n^{15/6}}{q^{3/2}} (\log n)^6 \max_i k_i^6. \tag{2.12}$$

The major arcs give rise to the following contribution towards (2.11),

$$\sum_{1 \leq q \leq n^\nu} \sum_{\substack{1 \leq c \leq q \\ \gcd(c,q)=1}} \int_{-q^{-1}n^{-2/3}}^{q^{-1}n^{-2/3}} f_{a_1,k_1}(c/q + \beta) f_{a_2,k_2}(c/q + \beta) f_{a_3,k_3}(c/q + \beta) e(-n(c/q + \beta)) d\beta,$$



and a straightforward analysis utilising (2.12) reveals that the last expression equals

$$\sum_{1 \leq q \leq n^v} \sum_{\substack{1 \leq c \leq q \\ \gcd(c,q)=1}} \frac{e_q(-cn)L_{\mathbf{a},q,\mathbf{k}}(c)}{d_{\mathbf{a},\mathbf{k}}(q)} \int_{-q^{-1}n^{-2/3}}^{q^{-1}n^{-2/3}} \left( \int_0^n e(\beta x) dx \right)^3 e(-n\beta) d\beta + O\left(\frac{n^{11/6}(\log n)^6}{\max_i k_i^{-6}}\right).$$

The integral over  $\beta$  can be estimated as  $n^2/2 + O(q^2n^{4/3})$ , thus by (2.10) the sum over  $q$  is  $\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)n^2/2 + O((n^{4/3+v} + n^{2-v})(\log n)^3)$  and the choice  $v = 1/6$  concludes the proof of Proposition 2.1.

### 3. Fusing the circle method with Hooley's approach

#### 3.1. Opening phase

The aim of Section 3 is to prove Theorem 1.1 and Theorem 1.3. We commence in this subsection by calling upon parts of Hooley's work [7] that will prove useful. We will make an effort to keep the notation in line with his as much as possible. In this section, the letters  $p, q$  will be reserved for primes. Two primes  $p, q$  are said to satisfy the property  $R_a(q, p)$  if both of the following conditions hold,

$$q|(p - 1); a \text{ is a } q\text{th power residue (mod } p).$$

A standard index calculus argument shows that for a prime  $p \nmid a$  the integer  $a$  is a primitive root (mod  $p$ ) if and only if  $R_a(q, p)$  fails for all primes  $q$ . For any  $\eta, \eta_1, \eta_2 \in \mathbb{R}_{>0}$  we define

$$N_a(n, \eta) := \#\{p \leq n : R_a(q, p) \text{ fails for all primes } q \leq \eta\}$$

and

$$M_a(n, \eta_1, \eta_2) := \#\{p \leq n : \text{there exists } q \in (\eta_1, \eta_2] \text{ such that } R_a(q, p) \text{ holds}\}.$$

Letting

$$N_a(n) := \#\{p \leq n : a \text{ is a primitive root modulo } p\}$$

we see from the work of Hooley [7, equation (1)] that for each  $\xi_1, \xi_2, \xi_3 \in \mathbb{R}$  with

$$1 \leq \xi_1 < \xi_2 < \xi_3 < n - 1$$

we have

$$N_a(n) = N_a(n, \xi_1) + O(M_a(n, \xi_1, \xi_2) + M_a(n, \xi_2, \xi_3) + M_a(n, \xi_3, n - 1)).$$

Hooley makes specific choices for the parameters  $\xi_i$ ; we will keep the same choice for  $\xi_2$  and  $\xi_3$ , namely  $\xi_2 := n^{1/2}(\log n)^{-2}$ ,  $\xi_3 := n^{1/2} \log n$ , however, we shall later choose a different value for  $\xi_1$ . For the moment we shall only demand that  $1 < \xi_1 \leq (\log n)(\log \log n)^{-1}$ . The estimates proved in [7, equations (2) and (3)] provide us with

$$N_a(n) = N_a(n, \xi_1) + O(M_a(n, \xi_1, \xi_2) + n(\log \log n)(\log n)^{-2}). \tag{3.1}$$

The argument in [7, equation (33)] shows that for each  $\xi_1$  as above, one has under HRH( $a$ ) that

$$M_a(n, \xi_1, \xi_2) \ll \frac{n}{\log n} \sum_{q > \xi_1} \frac{1}{q^2} + \frac{n}{\log^2 n},$$

which, once combined with the simple estimate  $\sum_{q>\xi_1} q^{-2} \ll \xi_1^{-1}$  and (3.1) provides us with

$$N_a(n) = N_a(n, \xi_1) + O\left(\frac{n}{\log n} \frac{1}{\xi_1} + \frac{n \log \log n}{\log^2 n}\right), \tag{3.2}$$

with an implied constant depending at most on  $a$ .

LEMMA 3.1. *For any  $\beta \in (0, 1)$  and any sets of primes  $\mathcal{P}_i \subset [1, n]$  of cardinality  $\varepsilon(\mathcal{P}_i)n/\log n$  the following estimate holds with an implied constant that depends at most on  $\beta$ ,*

$$\sum_{\substack{p_1+p_2+p_3=n \\ \exists i: p_i \in \mathcal{P}_i}} \prod_{i=1}^3 \log p_i \ll_{\beta} n^2 (\max_i \varepsilon(\mathcal{P}_i))^{\beta}.$$

*Proof.* Define  $r_2(m) := \#\{(p_1, p_2) : p_i \text{ prime, } p_1 + p_2 = m\}$ . The sum in the lemma is at most

$$(\log n)^3 \sum_{i=1}^3 \sum_{\substack{p_1+p_2+p_3=n \\ p_i \in \mathcal{P}_i}} 1 = (\log n)^3 \sum_{i=1}^3 \sum_{p < n} \mathbf{1}_{\mathcal{P}_i}(p) r_2(n - p)$$

and using Hölder’s inequality with exponents  $(1/\beta, 1/(1 - \beta))$  allows us to bound the inner sum on the right by

$$\varepsilon(\mathcal{P}_i)^{\beta} n^{\beta} (\log n)^{-\beta} \left( \sum_{p < n} r_2(n - p)^{1/(1-\beta)} \right)^{1-\beta}.$$

Straightforwardly, there exists  $c = c(\beta) > 0$  with  $(1 - z)/(1 - 2z) \leq (1 + cz)^{1-\beta}$  for all  $0 < z \leq 1/3$ . Using this for  $z = 1/p'$  and alluding to the following classical bound (that can be found in [3, equation (7.2)], for example),

$$r_2(m) \ll \frac{m}{(\log m)^2} \prod_{p'|m, p' \neq 2} \frac{p' - 1}{p' - 2}$$

yields

$$r_2(m) \ll_{\beta} \frac{m}{(\log m)^2} \prod_{p'|m} \left(1 + \frac{c}{p'}\right)^{1-\beta}.$$

Therefore the quantity in the lemma is

$$\ll (\log n)^3 \left(\frac{n \max_i \varepsilon(\mathcal{P}_i)}{\log n}\right)^{\beta} \left(\frac{n}{(\log n)^2}\right)^{1/(1-\beta)} \sum_{p < n} \prod_{p'|n-p} (1 + c/p')$$

and to finish our proof it remains to show that

$$\sum_{p < n} \prod_{p'|n-p} (1 + c/p') \ll_c \frac{n}{\log n}.$$

Rewriting this sum as  $\sum_{d \leq n} \mu(d)^2 c^{\omega(d)} d^{-1} \#\{p < n : p \equiv n \pmod{d}\}$  we see that the contribution from the integers  $d > n^{1/2}$  is  $\ll \sum_{n^{1/2} < d \leq n} c^{\omega(d)} d^{-1} (n/d + 1) \ll n^{1/2+1/100}$ . By the Brun–Titchmarsh theorem, the terms with  $d \leq n^{1/2}$  contribute  $\ll n(\log n)^{-1} \sum_{d \leq n^{1/2}} c^{\omega(d)} (d\varphi(d))^{-1} \ll n(\log n)^{-1}$ , thus concluding our proof.

Let us define the set

$$\mathcal{P}_i := \{p : p|a_i\} \cup \{p \leq n : R_{a_i}(q, p) \text{ holds for some prime } q > \xi_1\}.$$

The arguments bounding  $M_a(n, \xi_1, n - 1)$  in the deduction of (3.2) show under HRH( $a$ ) that

$$\#\mathcal{P}_i \ll \frac{n}{\xi_1 \log n} + \frac{n \log \log n}{\log^2 n}. \tag{3.3}$$

By (3.3) we have

$$\varepsilon(\mathcal{P}_i) = \frac{\log n}{n} \#\mathcal{P}_i \ll \frac{1}{\xi_1} + \frac{\log \log n}{\log n} \ll \frac{1}{\xi_1},$$

and thus we can apply Lemma 3.1. Therefore, under HRH( $a_i$ ) for  $i = 1, 2, 3$ , and for each fixed  $\beta \in (0, 1)$  we obtain the validity of

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i: \mathbb{F}_{p_i}^* = \langle a_i \rangle}} \prod_{i=1}^3 \log p_i = \sum_{\substack{p_1+p_2+p_3=n, p_i \nmid a_i \\ \forall i, \forall q \leq \xi_1: R_{a_i}(q, p_i) \text{ fails}}} \prod_{i=1}^3 \log p_i + O_\beta\left(\frac{n^2}{\xi_1^\beta}\right).$$

Bringing into play the following quantity for each square-free positive integer  $k_i$ ,

$$P_{\mathbf{a}, \mathbf{k}}(n) := \sum_{\substack{p_1+p_2+p_3=n, p_i \nmid a_i \\ \forall i: q|k_i \Rightarrow R_{a_i}(q, p_i) \text{ holds}}} \prod_{i=1}^3 \log p_i, \tag{3.4}$$

makes the following estimate available, once the inclusion-exclusion principle has been used,

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i: \mathbb{F}_{p_i}^* = \langle a_i \rangle}} \prod_{i=1}^3 \log p_i = \sum_{\substack{\mathbf{k} \in \mathbb{N}^3 \\ p|k_1 k_2 k_3 \Rightarrow p \leq \xi_1}} \mu(k_1)\mu(k_2)\mu(k_3) P_{\mathbf{a}, \mathbf{k}}(n) + O_\beta\left(n^2 \xi_1^{-\beta}\right). \tag{3.5}$$

The entity  $P_{\mathbf{a}, \mathbf{k}}(n)$  is analogous to  $P_a(k)$  that is present in the work of Hooley [7, section 3]. Indeed, the inclusion-exclusion argument above is inspired by the argument leading to [7, equation (5)].

Using the arguments in [7, section 4] we shall first translate the  $R_{a_i}(q, p_i)$ -condition present in (3.4) into a condition related to the factorisation properties of the prime  $p_i$  in certain number fields. Recall the definition of  $h_a$  given in (1.3). For any positive square-free integer  $k_i$  we define  $k'_i := k_i / \gcd(k_i, h_{a_i})$ . Then, as explained in [7, equation (8)], for a prime  $p \nmid a_i$  and a square-free integer  $k_i$ , the conditions  $R_{a_i}(q, p)$  hold for all  $q | k_i$  if and only if

$$x^{k'_i} \equiv a_i \pmod{p} \text{ is soluble and } p \equiv 1 \pmod{k_i}.$$

It is then proved following [7, Eq.(8)] that, in light of the Kummer–Dedekind theorem, this is in turn equivalent to the property that  $p$  is completely split in the number field  $\mathbb{Q}(a_i^{1/k_i}, \zeta_{k_i})$ . Recall (1.1) and let us see why

$$G_{a_i, k_i} = \mathbb{Q}(a_i^{1/k_i}, \zeta_{k_i}).$$

It is clearly sufficient to show that  $a_i^{1/k_i} \in \mathbb{Q}(a_i^{1/k_i'}, \zeta_{k_i})$ . Writing  $a_i = b^{h_{a_i}}$  and using  $\mu(k_i)^2 = 1$ , we see that  $\gcd(h_{a_i} \gcd(k_i, h_{a_i}), k_i) | h_{a_i}$ , hence there are integers  $x, y$  with

$$h_{a_i} \gcd(k_i, h_{a_i})x + k_i y = h_{a_i}.$$

This leads to the equality  $a_i^{1/k_i} = (b^{1/k_i})^{h_{a_i}} = b^y (a_i^{1/k_i'})^x$ , which completes the argument.

Recalling the definition of  $\text{Spl}(G_{a_i, k_i})$  in (2.1), we infer by (3.4) that for all  $\mathbf{k} \in \mathbb{N}^3$  with each  $k_i$  square-free we have

$$P_{\mathbf{a}, \mathbf{k}}(n) = \sum_{\substack{p_1+p_2+p_3=n, p_i \nmid a_i \\ \forall i: p_i \in \text{Spl}(G_{a_i, k_i})}} \prod_{i=1}^3 \log p_i = V_{\mathbf{a}, \mathbf{k}}(n) + O_\beta(n^2((\log n)/n)^\beta),$$

for any  $\beta \in (0, 1)$ . For the second equality, recall (2.2) and use Lemma 3.1. Inserting this into (3.5) we have proved that whenever  $1 < \xi_1 \leq (\log n)(\log \log n)^{-1}$  and  $0 < \beta < 1$ , then

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i: p_i^* = \langle a_i \rangle}} \prod_{i=1}^3 \log p_i = \sum_{\substack{\mathbf{k} \in \mathbb{N}^3 \\ p | k_1 k_2 k_3 \Rightarrow p \leq \xi_1}} \mu(k_1)\mu(k_2)\mu(k_3) V_{\mathbf{a}, \mathbf{k}}(n) + O_\beta(n^2 \xi_1^{-\beta}). \tag{3.6}$$

For summing up the error terms, we have used the following estimate, valid for  $2 - \beta < \delta < 2$ ,

$$\begin{aligned} \sum_{\substack{\mathbf{k} \in \mathbb{N}^3 \\ p | k_1 k_2 k_3 \Rightarrow p \leq \xi_1}} |\mu(k_1)\mu(k_2)\mu(k_3)| n^\delta &\leq n^\delta \left( \sum_{\substack{k \in \mathbb{N} \\ p | k \Rightarrow p \leq \xi_1}} |\mu(k)| \right)^3 = n^\delta 2^{3\#\{p \leq \xi_1\}} \\ &\leq n^\delta e^{3\xi_1} \leq n^{\delta + \frac{3}{\log \log n}} \\ &\ll_{\beta, \delta} n^2 (\log n)^{-\beta} (\log \log n)^\beta \leq n^2 \xi_1^{-\beta}. \end{aligned}$$

Before concluding the proofs of Theorem 1.1 and Theorem 1.3, we need a preparatory lemma.

LEMMA 3.2. *The series defining  $\mathfrak{S}_{\mathbf{a}, \mathbf{k}}(n)$  in (1.10) and the series representing  $\mathcal{A}_{\mathbf{a}}(n)$  in (1.11) are absolutely convergent. For each  $\varepsilon > 0$  and  $z \geq 1$  we have*

$$\sum_{\substack{\mathbf{k} \in \mathbb{N}^3 \\ \exists i, p: p | k_i \text{ and } p \geq z}} |\mathfrak{S}_{\mathbf{a}, \mathbf{k}}(n)| \left( \prod_{i=1}^3 |\mu(k_i)| \right) \leq \sum_{\substack{\mathbf{k} \in \mathbb{N}^3 \\ \exists i: k_i \geq z}} \left( \prod_{i=1}^3 |\mu(k_i)| \right) \sum_{q=1}^\infty \frac{1}{d_{\mathbf{a}, \mathbf{k}}(q)} \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^*} |L_{\mathbf{a}, q, \mathbf{k}}(x)| \ll_\varepsilon \frac{1}{z^{1-\varepsilon}},$$

with an implied constant depending at most on  $\mathbf{a}$  and  $\varepsilon$ .

*Proof.* The first inequality is clear by (1.10). Observe that  $k'_i \geq k_i/h_{a_i} \gg k_i$ , hence by Lemma 2.2 we obtain

$$\frac{1}{d_{\mathbf{a},\mathbf{k}}(q)} \ll \prod_{i=1}^3 \frac{1}{k_i \varphi([q, k_i])} = \frac{1}{\varphi(q)^3} \prod_{i=1}^3 \frac{\varphi(\gcd(q, k_i))}{k_i \varphi(k_i)}.$$

Combining this with (2.10) we see by (1.10) that for  $\varepsilon > 0$  and square-free  $k_i$ ,

$$\begin{aligned} \sum_{q=1}^{\infty} \frac{1}{d_{\mathbf{a},\mathbf{k}}(q)} \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^*} |L_{\mathbf{a},q,\mathbf{k}}(x)| &\ll \prod_{i=1}^3 \frac{1}{k_i \varphi(k_i)} \sum_{q=1}^{\infty} \frac{\varphi(\gcd(q, k_1)) \varphi(\gcd(q, k_2)) \varphi(\gcd(q, k_3))}{\varphi(q)^2} \\ &\ll_{\varepsilon} \frac{\gcd(k_1, k_2, k_3)}{(k_1 k_2 k_3)^{2-\varepsilon}}. \end{aligned}$$

Therefore, the inner sum in our lemma satisfies the bound

$$\ll \sum_{k_1 \geq z} \frac{|\mu(k_1)|}{k_1^{2-\varepsilon}} \sum_{k_2 \in \mathbb{N}} \frac{|\mu(k_2)|}{k_2^{2-\varepsilon}} \sum_{k_3 \in \mathbb{N}} \frac{|\mu(k_3)| \gcd(k_1, k_2, k_3)}{k_3^{2-\varepsilon}}.$$

We conclude the proof of our desired bound using the estimates

$$\sum_{k_3 \in \mathbb{N}} |\mu(k_3)| \gcd(k_3, m) k_3^{-2+\varepsilon} \ll_{\varepsilon} m^{\varepsilon} \quad \text{and} \quad \sum_{k_1 \geq z} \frac{|\mu(k_1)|}{k_1^{2-\varepsilon}} \ll z^{-1+\varepsilon}.$$

This bound implies in particular the absolute convergence of the sum in (1.11).

### 3.2. The proof of Theorem 1.1

Recall (2.3). Now note that, replacing  $f_{\mathbf{a}}(\mathbf{x})$  by a larger function if necessary, we may assume in the statement of (2.3) that  $f_{\mathbf{a}}([1, \infty)^3)$  is a subset of  $(1, \infty)$ . Fix any  $B > 0$ . The function

$$x \mapsto \log(1+x) + \sum_{1 \leq k_1, k_2, k_3 \leq x} f_{\mathbf{a}}(\mathbf{k}),$$

is strictly increasing, hence it has an inverse, say  $h_{\mathbf{a}}(x)$ . Define the function  $\xi_1 : (1, \infty) \rightarrow \mathbb{R}$  through

$$\xi_1(x) := \frac{1}{2} \cdot \min \left\{ \frac{\log x}{\log \log x}, \log(h_{\mathbf{a}}((\log x)^{B/2})) \right\} \tag{3.7}$$

and observe that

$$\lim_{x \rightarrow +\infty} \xi_1(x) = +\infty, \tag{3.8}$$

however, owing to the non-explicit error term in [9, Theorem 2] we cannot have any further control on the rate of divergence in the last limit. For  $n \gg 1$ , the definition of  $\xi_1$  implies

$$\sum_{1 \leq k_1, k_2, k_3 \leq e^{2\xi_1(n)}} f_{\mathbf{a}}(\mathbf{k}) \leq (\log n)^{B/2}.$$

Noting that a square-free integer with all of its prime factors bounded by  $\xi_1(n)$  must be at most  $\prod_{p \leq \xi_1(n)} p \leq \exp(2\xi_1(n))$  and inserting (2.3) into (3.6) yields the following with an

implied constant depending on  $\beta$  and  $B$ ,

$$\begin{aligned} \sum_{\substack{p_1+p_2+p_3=n \\ \forall i: \mathbb{F}_{p_i}^* = \langle a_i \rangle}} \prod_{i=1}^3 \log p_i &= \frac{n^2}{2} \sum_{\substack{\mathbf{k} \in \mathbb{N}^3 \\ p|k_1 k_2 k_3 \Rightarrow p \leq \xi_1(n)}} \left( \prod_{i=1}^3 \mu(k_i) \right) \mathfrak{S}_{\mathbf{a}, \mathbf{k}}(n) \\ &\quad + O\left( \frac{n^2}{\xi_1^\beta} + \frac{n^2}{(\log n)^B} \left( \sum_{\substack{\mathbf{k} \in \mathbb{N}^3 \\ \forall i: k_i \leq e^{2\xi_1(n)}}} f_{\mathbf{a}}(\mathbf{k}) \right) \right) \\ &= \frac{n^2}{2} \sum_{\substack{\mathbf{k} \in \mathbb{N}^3 \\ p|k_1 k_2 k_3 \Rightarrow p \leq \xi_1(n)}} \left( \prod_{i=1}^3 \mu(k_i) \right) \mathfrak{S}_{\mathbf{a}, \mathbf{k}}(n) + O\left( \frac{n^2}{\xi_1^\beta} + \frac{n^2}{(\log n)^{B/2}} \right). \end{aligned}$$

An application of Lemma 3.2 with  $\varepsilon = 1 - \beta$  shows that

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i: \mathbb{F}_{p_i}^* = \langle a_i \rangle}} \prod_{i=1}^3 \log p_i - \frac{1}{2} \left( \sum_{\mathbf{k} \in \mathbb{N}^3} \mu(k_1) \mu(k_2) \mu(k_3) \mathfrak{S}_{\mathbf{a}, \mathbf{k}}(n) \right) n^2 \ll_{\beta, B} \frac{n^2}{\min\{(\log n)^{B/2}, \xi_1(n)^\beta\}},$$

and the proof of Theorem 1.1 is concluded upon invoking (3.8), except for the assertion that  $\mathcal{A}_{\mathbf{a}}(n) \gg_a 1$  whenever  $\mathcal{A}_{\mathbf{a}}(n) > 0$ . This assertion follows immediately from Theorem 1.5, proved in Section 4. Moreover, we have confirmed the shape of  $\mathcal{A}_{\mathbf{a}}(n)$  given in (1.11).

Note that the reason for the non-explicit error term in Theorem 1.1 is that the function  $\xi_1$  in (3.7) is not explicit.

### 3.3. The proof of Theorem 1.3

Let  $\beta$  be any real number in  $(0, 1)$  and define

$$\xi_1(n) := \frac{\log n}{\log \log n}.$$

We insert in (3.6) the estimate for  $V_{\mathbf{a}, \mathbf{k}}(n)$  given in Proposition 2.1 to see that

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i: \mathbb{F}_{p_i}^* = \langle a_i \rangle}} \prod_{i=1}^3 \log p_i - \frac{n^2}{2} \sum_{p|k_1 k_2 k_3 \Rightarrow p \leq \xi_1} \mathfrak{S}_{\mathbf{a}, \mathbf{k}}(n) \prod_{i=1}^3 \mu(k_i) \ll_{\beta} \frac{n^2}{\xi_1^\beta} + \frac{(\log n)^6}{n^{-11/6}} \left( \sum_{\substack{k \in \mathbb{N} \\ p|k \Rightarrow p \leq \xi_1}} k^6 |\mu(k)| \right)^3.$$

For  $n \gg 1$ , each  $k$  in the sum satisfies  $k \leq \prod_{p \leq \xi_1} p \leq n^{\frac{2}{\log \log n}}$ , hence the cube of the sum over  $k$  is at most  $n^{\frac{\theta}{\log \log n}}$  for some absolute positive constant  $\theta$ . This shows that the right-hand side above is  $\ll_{\beta} n^2 \xi_1^{-\beta}$ . Appealing to Lemma 3.2 completes the proof of Theorem 1.3.

## 4. Artin’s factor for ternary Goldbach

In this section, we study in detail the leading factor  $\mathcal{A}_{\mathbf{a}}(n)$  in Theorems 1.1 and 1.3, and thus prove Theorem 1.5, Corollary 1.6 and Theorem 1.7. Recall that we have already confirmed the equality (1.11) in the proof of Theorem 1.1 in Section 3.2.

### 4.1. The proof of (1.14)

Recall the definitions of  $F_{a,q,k}(b)$  and  $c_{a,q,k}(b)$  from the start of Section 1.3. It was shown by Lenstra [10, theorem (3.1), equation (2.15)] conditionally under HRH( $a$ ), that for all

integers  $b$  and  $q > 0$  the natural density of the primes  $p$  satisfying the following conditions exists,

$$\mathbb{F}_p^* = \langle a \rangle \text{ and } p \equiv b \pmod{q},$$

and, furthermore, that it equals  $\sum_{k \in \mathbb{N}} \mu(k) c_{a,q,k}(b) [F_{a,q,k} : \mathbb{Q}]^{-1}$ . This topic was later revisited by Moree [12], who showed that

$$\sum_{k \in \mathbb{N}} \frac{\mu(k) c_{a,q,k}(b)}{[F_{a,q,k} : \mathbb{Q}]} = \delta_a(b \pmod{q}), \tag{4.1}$$

where  $\delta_a(b \pmod{q})$  is the arithmetic function given in Definition 1.4. We will make consequent use of Moree's result in this section.

LEMMA 4.1. *We have*

$$\sum_{\mathbf{k} \in \mathbb{N}^3} \mu(k_1) \mu(k_2) \mu(k_3) \mathfrak{S}_{\mathbf{a}, \mathbf{k}}(n) = \sum_{q=1}^{\infty} \sum_{c \in (\mathbb{Z}/q\mathbb{Z})^*} e_q(-nc) \prod_{i=1}^3 \left( \sum_{b_i \in \mathbb{Z}/q\mathbb{Z}} e_q(b_i c) \delta_{a_i}(b_i \pmod{q}) \right).$$

*Proof.* Recall (1.9) and (1.10). Lemma 3.2 allows us to rearrange terms, thus we can rewrite the sum over  $\mathbf{k}$  in our lemma as

$$\sum_{q=1}^{\infty} \sum_{\substack{c \in \mathbb{Z}/q\mathbb{Z} \\ \gcd(c,q)=1}} e_q(-cn) \prod_{i=1}^3 \left( \sum_{k_i \in \mathbb{N}} \frac{\mu(k_i) S_{a_i,q,k_i}(c)}{[F_{a_i,q,k_i} : \mathbb{Q}]} \right).$$

By (1.9) the sum over  $k_i$  equals

$$\sum_{\substack{b_i \in \mathbb{Z}/q\mathbb{Z} \\ \gcd(b_i,q)=1}} e_q(b_i c) \sum_{k_i \in \mathbb{N}} \frac{\mu(k_i) c_{a_i,q,k_i}(b_i)}{[F_{a_i,q,k_i} : \mathbb{Q}]}$$

and using (4.1) concludes our proof.

The difficulty of converting the sum over  $\mathbf{k}$  in (1.11) into a product comes from the fact that the terms  $\delta_{a_i}(b_i \pmod{q})$  in Lemma 4.1 are not a multiplicative function of  $q$ . These terms would be multiplicative in the classical Vinogradov setting, where one has  $\mathbf{1}_{\gcd(b_i,q)=1}(b_i) / \varphi(q)$  in place of  $\delta_{a_i}(b_i \pmod{q})$ .

For brevity, we will write from now on  $\beta_i(q)$  and  $\Delta_i$  for  $\beta_{a_i}(q)$  and  $\Delta_{a_i}$ .

LEMMA 4.2. *If the odd part of a positive integer  $q$  is not square-free then the following expression vanishes,*

$$\prod_{i=1}^3 \left( \sum_{b_i \in \mathbb{Z}/q\mathbb{Z}} e_q(b_i c) \delta_{a_i}(b_i \pmod{q}) \right).$$

*The expression also vanishes if  $v_2(q) > \min\{v_2(\Delta_i) : i = 1, 2, 3\}$ .*

*Proof.* In the present proof we write  $[P] := 1$  if a proposition  $P$  holds, and  $[P] := 0$  otherwise. For  $1 \leq i \leq 3$ , we factorise each positive integer  $q$  uniquely as  $q = q_{i,0} q_{i,1}$ , where  $q_{i,0}$  is only divisible by primes dividing  $\Delta_i$  and  $\gcd(q_{i,1}, \Delta_i) = 1$ . Now owing to Definition 1.4

the quantity  $\delta_{a_i}(b_i \bmod q)/\mathcal{A}_{a_i}$  equals

$$\begin{aligned} & \left( [\gcd(b_i, q_{i,1}) \gcd(b_i - 1, q_{i,1}, h_{a_i}) = 1] \frac{f_{a_i}^\dagger(q_{i,1})}{\varphi(q_{i,1})} \prod_{p|b_i-1, p|q_{i,1}} \left(1 - \frac{1}{p}\right) \right) \\ & \times \left( \frac{f_i^\dagger(q_{i,0})}{\varphi(q_{i,0})} \prod_{p|b_i-1, p|q_{i,0}} \left(1 - \frac{1}{p}\right) \right) [\gcd(b_i, q_{i,0}) \gcd(b_i - 1, q_{i,0}, h_{a_i}) = 1] \\ & \times \left( 1 + \left( \frac{\beta_i(q_{i,0})}{b_i} \right) \mu \left( \frac{2|\Delta_i|}{\gcd(q_{i,0}, \Delta_i)} \right) f_{a_i}^\ddagger \left( \frac{|\Delta_i|}{\gcd(q_{i,0}, \Delta_i)} \right) \right). \end{aligned}$$

The integers  $q_{i,0}$  and  $q_{i,1}$  are coprime, hence we may write  $b_i = q_{i,0}b_{i,1} + q_{i,1}b_{i,0}$  and use the Chinese remainder theorem to write the sum over  $b_i$  in the lemma as the product of

$$\mathcal{A}_{a_i} \cdot \frac{f_{a_i}^\dagger(q_{i,0})}{\varphi(q_{i,0})} \frac{f_{a_i}^\dagger(q_{i,1})}{\varphi(q_{i,1})} \sum_{\substack{b_{i,1} \pmod{q_{i,1}} \\ \gcd(b_{i,1}, q_{i,1})=1 \\ \gcd(b_{i,1}q_{i,0}-1, q_{i,1}, h_{a_i})=1}} e(b_{i,1}c/q_{i,1}) \prod_{p|(b_{i,1}q_{i,0}-1, q_{i,1})} \left(1 - \frac{1}{p}\right)$$

and

$$\begin{aligned} & \sum_{\substack{b_{i,0} \pmod{q_{i,0}} \\ \gcd(b_{i,0}, q_{i,0})=1 \\ \gcd(b_{i,0}q_{i,1}-1, q_{i,0}, h_{a_i})=1}} \frac{e(b_{i,0}c/q_{i,0})}{\prod_{p|(b_{i,0}q_{i,1}-1, q_{i,0})} (1 - \frac{1}{p})^{-1}} \left( 1 + \left( \frac{\beta_i(q_{i,0})}{b_{i,0}q_{i,1}} \right) \right) \\ & \times \mu \left( \frac{2|\Delta_i|}{\gcd(q_{i,0}, \Delta_i)} \right) f_{a_i}^\ddagger \left( \frac{|\Delta_i|}{\gcd(q_{i,0}, \Delta_i)} \right). \end{aligned}$$

To study the sum over  $b_{i,1}$  we use Lemma 2.13 with

$$Q := q_{i,1}, \quad r := \prod_{p|q_{i,1}} p, \quad f(b) := [\gcd(b, r) \gcd(b - 1, r, h_{a_i}) = 1] \prod_{p|b-1, p|r} \left(1 - \frac{1}{p}\right)$$

to deduce that if the expression in our lemma is non-vanishing then for each  $i$  the integer  $q_{i,1}$  must be square-free. Now assume that the prime  $p$  satisfies  $p \nmid \gcd(\Delta_1, \Delta_2, \Delta_3)$ . Then there exists  $i \in \{1, 2, 3\}$  such that  $p \nmid \Delta_i$  and then the non-vanishing of the expression in the lemma implies that  $q_{i,1}$  must be square-free, thus  $v_p(q) = v_p(q_{i,1}) \leq 1$ .

Now the sum over  $b_{i,0}$  can be studied via Lemma 2.13 with  $Q := q_{i,0}$ ,  $r := \gcd(q_{i,0}, \Delta_i)$  and with  $f(b)$  being the product of  $[\gcd(b, r) \gcd(bq_{i,1} - 1, r, h_{a_i}) = 1]$  and

$$\left\{ 1 + \left( \frac{\beta(q_{i,0})}{b} \right) \mu \left( \frac{2|\Delta_i|}{\gcd(q_{i,0}, \Delta_i)} \right) f_i^\ddagger \left( \frac{|\Delta_i|}{\gcd(q_{i,0}, \Delta_i)} \right) \right\} \prod_{p|(bq_{i,1}-1, r)} \left(1 - \frac{1}{p}\right).$$

We have used the fact that  $p | q_{i,0}$  if and only if  $p | r$ , and that the Kronecker symbol has period  $|\beta(q_{i,0})| = r$ . Lemma 2.13 shows that unless the expression in our lemma vanishes, we have  $\gcd(q_{i,0}, \Delta_i) = q_{i,0}$ , thus for every  $i$  we must have  $q_{i,0} | \Delta_i$ . Now if a prime  $p$  satisfies  $p | \gcd(\Delta_1, \Delta_2, \Delta_3)$  we have that for every  $i$ ,  $v_p(q) = v_p(q_{i,0}) \leq v_p(\Delta_i)$ , thus  $v_p(q) \leq \min\{v_p(\Delta_i) : i = 1, 2, 3\}$ . If  $p \neq 2$  then this shows that  $v_p(q) \leq 1$  since the odd part of a fundamental discriminant is square-free, while if  $p = 2$  then we must have  $v_2(q) \leq \min\{v_2(\Delta_i) : i = 1, 2, 3\}$ .



Lemma 4.2 allows us to simplify the summation over  $q$  in Lemma 4.1, since the only integers  $q$  making a contribution towards the sum must satisfy

$$\forall p, i : p|\Delta_i, p|q \Rightarrow v_p(q) \leq v_p(\Delta_i) \quad \text{and} \quad p|q, p \nmid \Delta_1 \Delta_2 \Delta_3 \Rightarrow v_p(q) \leq 1.$$

To keep track of every factorisation we introduce for every  $q \in \mathbb{N}$  and  $\mathbf{w} \in \{0, 1\}^3$  the positive integer

$$q(\mathbf{w}) := \prod_{\substack{p: \\ \forall i: p|\Delta_i \Leftrightarrow \mathbf{w}(i)=0}} p^{v_p(q)},$$

so that  $q = \prod_{\mathbf{w} \in \mathbb{F}_2^3} q(\mathbf{w})$ . Furthermore, whenever  $\mathbf{w} \neq \mathbf{u}$  then we have  $\gcd(q(\mathbf{w}), q(\mathbf{u})) = 1$ . Note that for a given  $q$ ,  $q(\mathbf{w})$  is uniquely characterised by the properties

$$\gcd(q(\mathbf{w}), \prod_{i:\mathbf{w}(i)=1} \Delta_i) = 1 \quad \text{and} \quad q(\mathbf{w}) \mid \gcd\{\Delta_i : \mathbf{w}(i) = 0\}. \tag{4.2}$$

In the case  $\mathbf{w} = (1, 1, 1)$ , the latter condition is interpreted as vacuous. It may be that for certain values of  $a_i$  and for all  $q$  some  $q(\mathbf{w})$  are equal to 1; for example, this happens if  $a_1 = a_2 = a_3$ , in which case we see that  $\mathbf{w} \notin \{(0, 0, 0), (1, 1, 1)\}$  implies that  $q(\mathbf{w}) = 1$ . We now use the definition of  $q(\mathbf{w})$ , Lemma 4.1 and Lemma 4.2 to infer

$$\begin{aligned} \sum_{\mathbf{k} \in \mathbb{N}^3} \mu(k_1)\mu(k_2)\mu(k_3)\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n) &= \sum_{\substack{(q(\mathbf{w})) \in \mathbb{N}^3, \\ \text{(4.2) holds} \\ \mu(q((1,1,1)))^2=1}} \sum_{\substack{c \pmod{\prod_{\mathbf{w}} q(\mathbf{w})} \\ \gcd(c, \prod_{\mathbf{w}} q(\mathbf{w}))=1}} e(-nc \prod_{\mathbf{w}} q(\mathbf{w})^{-1}) \\ &\times \prod_{i=1}^3 \left( \sum_{b_i \pmod{\prod_{\mathbf{w}} q(\mathbf{w})}} e\left(b_i c \prod_{\mathbf{w}} q(\mathbf{w})^{-1}\right) \right. \\ &\left. \times \delta_{a_i} \left( b_i \pmod{\prod_{\mathbf{w}} q(\mathbf{w})} \right) \right). \end{aligned} \tag{4.3}$$

Noting that the integers  $\prod_{\mathbf{w}(i)=0} q(\mathbf{w})$  and  $\prod_{\mathbf{w}(i)=1} q(\mathbf{w})$  are coprime, that

$$\gcd\left(\Delta_i, \prod_{\mathbf{w}} q(\mathbf{w})\right) = \prod_{\mathbf{w}(i)=0} q(\mathbf{w}),$$

and recalling Definition 1.4, we see that

$$\delta_{a_i} \left( b_i \pmod{\prod_{\mathbf{w}} q(\mathbf{w})} \right) = \delta_{a_i} \left( b_i \pmod{\prod_{\mathbf{w}(i)=0} q(\mathbf{w})} \right) \mathcal{A}_{a_i} \left( b_i \pmod{\prod_{\mathbf{w}(i)=1} q(\mathbf{w})} \right) \mathcal{A}_{a_i}^{-1}.$$

Writing  $b_i = b'_i \prod_{\mathbf{w}(i)=1} q(\mathbf{w}) + b''_i \prod_{\mathbf{w}(i)=0} q(\mathbf{w})$  and using the Chinese remainder theorem we obtain

$$\begin{aligned} &\sum_{b_i \pmod{\prod_{\mathbf{w}} q(\mathbf{w})}} e\left(b_i c \prod_{\mathbf{w}} q(\mathbf{w})^{-1}\right) \delta_{a_i} \left( b_i \pmod{\prod_{\mathbf{w}} q(\mathbf{w})} \right) \\ &= \sum_{b'_i \pmod{\prod_{\mathbf{w}(i)=0} q(\mathbf{w})}} e\left(b'_i c \prod_{\mathbf{w}(i)=0} q(\mathbf{w})^{-1}\right) \delta_{a_i} \left( b'_i \prod_{\mathbf{w}(i)=1} q(\mathbf{w}) \pmod{\prod_{\mathbf{w}(i)=0} q(\mathbf{w})} \right) \\ &\times \sum_{b''_i \pmod{\prod_{\mathbf{w}(i)=1} q(\mathbf{w})}} e\left(b''_i c \prod_{\mathbf{w}(i)=1} q(\mathbf{w})^{-1}\right) \mathcal{A}_{a_i}^{-1} \mathcal{A}_{a_i} \left( b''_i \prod_{\mathbf{w}(i)=0} q(\mathbf{w}) \pmod{\prod_{\mathbf{w}(i)=1} q(\mathbf{w})} \right). \end{aligned}$$

In order to analyse the expressions above, we introduce for  $r \in \mathbb{N}$ ,  $c \in \mathbb{Z}$  the quantity

$$\mathcal{M}_a(c, r) := \frac{1}{\mathcal{A}_a} \sum_{b \pmod{r}} e_r(bc) \mathcal{A}_a(b \pmod{r}) \tag{4.4}$$

and, for  $\mathbf{r} \in \mathbb{N}^k$ ,  $\mathbf{c} \in \mathbb{Z}^k$ , define

$$\mathcal{D}_a(\mathbf{c}, \mathbf{r}) := \sum_{b \pmod{r_1 \cdots r_k}} e \left[ b \left( \sum_{i=1}^k \frac{c_i}{r_i} \right) \right] \delta_a(b \pmod{r_1 \cdots r_k}).$$

Hence, writing

$$c = \sum_{\mathbf{w} \in \{0,1\}^3} c^{[\mathbf{w}]} \prod_{\mathbf{v} \neq \mathbf{w}} q(\mathbf{v}),$$

we see that  $\prod_{\mathbf{w}(i)=1} \mathcal{M}_{a_i}(c^{[\mathbf{w}]}, q(\mathbf{w}))$  equals

$$\mathcal{A}_{a_i}^{-1} \sum_{b'_i \pmod{\prod_{\mathbf{w}(i)=1} q(\mathbf{w})}} e \left( b'_i c \prod_{\mathbf{w}(i)=1} q(\mathbf{w})^{-1} \right) \mathcal{A}_{a_i} \left( b'_i \prod_{\mathbf{w}(i)=0} q(\mathbf{w}) \pmod{\prod_{\mathbf{w}(i)=1} q(\mathbf{w})} \right)$$

and that  $\mathcal{D}_{a_i}((c^{[\mathbf{w}]})_{\mathbf{w}(i)=0}, (q(\mathbf{w}))_{\mathbf{w}(i)=0})$  is

$$\sum_{b'_i \pmod{\prod_{\mathbf{w}(i)=0} q(\mathbf{w})}} e \left( b'_i c \prod_{\mathbf{w}(i)=0} q(\mathbf{w})^{-1} \right) \delta_{a_i} \left( b'_i \prod_{\mathbf{w}(i)=1} q(\mathbf{w}) \pmod{\prod_{\mathbf{w}(i)=0} q(\mathbf{w})} \right).$$

For  $\mathbf{w} = (1, 1, 1)$ , let  $\Delta_{\mathbf{w}} := 1$ . In case  $\mathbf{w} \neq (1, 1, 1)$ , we define

$$\Delta_{\mathbf{w}} := \prod_{p \mid \prod_{\mathbf{w}(i)=1} \Delta_i} p^{\min\{v_p(\Delta_i) : \mathbf{w}(i)=0\}}.$$

Then  $\prod_{\mathbf{w}} \Delta_{\mathbf{w}}$  coincides with the entity  $\mathfrak{D}_a$  introduced in (1.13). We see that the sum in (4.3) becomes

$$\begin{aligned} & \sum_{\substack{(q(\mathbf{w})) \in \mathbb{N}^8 \\ \mathbf{w} \neq (1,1,1) \Rightarrow q(\mathbf{w}) \mid \Delta_{\mathbf{w}} \\ \mu(q((1,1,1)))^2 = 1 \\ \gcd(q((1,1,1)), \Delta_1 \Delta_2 \Delta_3) = 1}} \sum_{(c^{[\mathbf{w}]} \in \prod_{\mathbf{w}} (\mathbb{Z}/q(\mathbf{w})\mathbb{Z})^* \quad \mathbf{w}} \left( \prod_{\mathbf{w}} e_{q(\mathbf{w})}(-nc^{[\mathbf{w}]}) \right) \\ & \times \prod_{i=1}^3 \left\{ \mathcal{D}_{a_i}((c^{[\mathbf{w}]})_{\mathbf{w}(i)=0}, (q(\mathbf{w}))_{\mathbf{w}(i)=0}) \prod_{\mathbf{w}(i)=1} \mathcal{M}_{a_i}(c^{[\mathbf{w}]}, q(\mathbf{w})) \right\}. \end{aligned}$$

Clearly, the terms corresponding to  $q((1, 1, 1))$  can be separated, thus, in light of (4.3), we are led to

$$\sum_{\mathbf{k} \in \mathbb{N}^3} \mu(k_1) \mu(k_2) \mu(k_3) \mathfrak{S}_{\mathbf{a}, \mathbf{k}}(n) = S_{\mathbf{a}, 0}(n) S_{\mathbf{a}, 1}(n), \tag{4.5}$$

where

$$S_{a,0}(n) := \sum_{\substack{(q(\mathbf{w}))_{\mathbf{w} \neq (1,1,1)} \in \mathbb{N}^7 \\ q(\mathbf{w}) | \Delta_{\mathbf{w}}}} \sum_{(c^{[\mathbf{w}]}) \in \prod_{\mathbf{w} \neq (1,1,1)} (\mathbb{Z}/q(\mathbf{w})\mathbb{Z})^*} \left( \prod_{\mathbf{w} \neq (1,1,1)} e_{q(\mathbf{w})}(-nc^{[\mathbf{w}]}) \right) \\ \times \prod_{i=1}^3 \left\{ \mathcal{D}_{a_i}((c^{[\mathbf{w}]})_{\mathbf{w}(i)=0}, (q(\mathbf{w}))_{\mathbf{w}(i)=0}) \prod_{\substack{\mathbf{w}(i)=1 \\ \mathbf{w} \neq (1,1,1)}} \mathcal{M}_{a_i}(c^{[\mathbf{w}]}, q(\mathbf{w})) \right\}$$

and

$$S_{a,1}(n) := \sum_{\gcd(q((1,1,1)), \Delta_1 \Delta_2 \Delta_3) = 1} \mu(q((1,1,1)))^2 \\ \times \sum_{c^{[(1,1,1)]} \in (\mathbb{Z}/q((1,1,1))\mathbb{Z})^*} e_{q((1,1,1))}(-nc^{[(1,1,1)]}) \prod_{i=1}^3 \mathcal{M}_{a_i}(c^{[(1,1,1)]}, q((1,1,1))). \tag{4.6}$$

LEMMA 4.3. For any  $q \in \mathbb{N}$  and  $\mathbf{w} \in \{0, 1\}^3$  define  $d_{\mathbf{w}} := \Delta_{\mathbf{w}}/q(\mathbf{w})$ .

(1) Let  $i \in \{1, 2, 3\}$  and for each  $\mathbf{w}$  with  $\mathbf{w}(i) = 0$  let  $c^{[\mathbf{w}]} \in (\mathbb{Z}/q(\mathbf{w})\mathbb{Z})^*$ . Then

$$\mathcal{D}_{a_i}((c^{[\mathbf{w}]})_{\mathbf{w}(i)=0}, (q(\mathbf{w}))_{\mathbf{w}(i)=0}) = \mathcal{D}_{a_i}((c^{[\mathbf{w}]}d_{\mathbf{w}})_{\mathbf{w}(i)=0}, (\Delta_{\mathbf{w}})_{\mathbf{w}(i)=0}).$$

(2) Let  $i \in \{1, 2, 3\}$ ,  $\mathbf{w} \in \{0, 1\}^3 \setminus \{(1, 1, 1)\}$  with  $\mathbf{w}(i) = 1$  and  $c^{[\mathbf{w}]} \in (\mathbb{Z}/q(\mathbf{w})\mathbb{Z})^*$ . Then

$$\mathcal{M}_{a_i}(c^{[\mathbf{w}]}, q(\mathbf{w})) = \mathcal{M}_{a_i}(c^{[\mathbf{w}]}d_{\mathbf{w}}, \Delta_{\mathbf{w}}).$$

Proof. (1) Define

$$Q := \prod_{\mathbf{w}: \mathbf{w}(i)=0} q(\mathbf{w}) = \prod_{\mathbf{w}: \mathbf{w}(i)=0} \frac{\Delta_{\mathbf{w}}}{d_{\mathbf{w}}} \text{ and } D := \prod_{\mathbf{w}: \mathbf{w}(i)=0} \Delta_{\mathbf{w}}.$$

If we assume HRH( $a_i$ ) then it is immediately clear from Moree's interpretation of  $\delta_{a_i}$  as densities [12] that the following holds,

$$\delta_{a_i}(m \bmod Q) = \sum_{\substack{b \pmod{D} \\ b \equiv m \pmod{Q}}} \delta_{a_i}(b \bmod D).$$

One can also prove this unconditionally directly from Definition 1.4 via a tedious but straightforward calculation that we do not reproduce here. To conclude the proof we observe that

$$\mathcal{D}_{a_i}((c^{[\mathbf{w}]})_{\mathbf{w}(i)=0}, (q(\mathbf{w}))_{\mathbf{w}(i)=0}) = \sum_{m \pmod{Q}} e\left(m \sum_{\mathbf{w}: \mathbf{w}(i)=0} \frac{c^{[\mathbf{w}]}}{q(\mathbf{w})}\right) \delta_{a_i}(m \bmod Q) \\ = \sum_{b \pmod{D}} e\left(b \sum_{\mathbf{w}: \mathbf{w}(i)=0} \frac{c^{[\mathbf{w}]}d_{\mathbf{w}}}{\Delta_{\mathbf{w}}}\right) \delta_{a_i}(b \bmod D) \\ = \mathcal{D}_{a_i}((c^{[\mathbf{w}]}d_{\mathbf{w}})_{\mathbf{w}(i)=0}, (\Delta_{\mathbf{w}})_{\mathbf{w}(i)=0}).$$

(2) Since by assumption  $\mathbf{w}(i) = 1$ , we have  $\gcd(\Delta_{\mathbf{w}}, \Delta_i) = 1$ , and thus,

$$\frac{\mathcal{A}_{a_i}(m \bmod \Delta_{\mathbf{w}})}{\mathcal{A}_{a_i}} = \frac{\delta_{a_i}(m \bmod \Delta_{\mathbf{w}})}{\mathcal{L}_{a_i}}.$$

We similarly have

$$\frac{\mathcal{A}_{a_i}(m \bmod \Delta_{\mathbf{w}}/d_{\mathbf{w}})}{\mathcal{A}_{a_i}} = \frac{\delta_{a_i}(m \bmod \Delta_{\mathbf{w}}/d_{\mathbf{w}})}{\mathcal{L}_{a_i}}.$$

By HRH( $a_i$ ) it then follows that

$$\mathcal{A}_{a_i}(m \bmod \Delta_{\mathbf{w}}/d_{\mathbf{w}}) = \sum_{\substack{b \pmod{\Delta_{\mathbf{w}}} \\ b \equiv m \pmod{\Delta_{\mathbf{w}}/d_{\mathbf{w}}}}} \mathcal{A}_{a_i}(b \bmod \Delta_{\mathbf{w}}),$$

which can also be shown unconditionally as above. The rest of the proof is carried out as in the first part.

For the analysis of  $S_{\mathbf{a},1}(n)$ , we recall the definition of  $\sigma_{\mathbf{a},n}(d)$  in (1.12) and use the following lemma.

LEMMA 4.4. *If  $p \nmid \Delta_1 \Delta_2 \Delta_3$ , then*

$$\sigma_{\mathbf{a},n}(p) = 1 + \sum_{c \in (\mathbb{Z}/p\mathbb{Z})^*} e_p(-nc) \prod_{i=1}^3 \mathcal{M}_{a_i}(c, p).$$

*Proof.* The easily verified equality  $\sum_{b \pmod{p}} \mathcal{A}_{a_i}(b \bmod p) = \mathcal{A}_{a_i}$  shows that the expression on the right-hand side is equal to

$$\begin{aligned} \sum_{c \in \mathbb{Z}/p\mathbb{Z}} e_p(-cn) \prod_{i=1}^3 \mathcal{M}_{a_i}(c, p) &= \sum_{\mathbf{b} \in (\mathbb{Z}/p\mathbb{Z})^3} \left( \prod_{i=1}^3 \frac{\mathcal{A}_{a_i}(b_i \bmod p)}{\mathcal{A}_{a_i}} \right) \sum_{c \in \mathbb{Z}/p\mathbb{Z}} e_p(c(b_1 + b_2 + b_3 - n)) \\ &= p \sum_{\substack{\mathbf{b} \in (\mathbb{Z}/p\mathbb{Z})^3 \\ \sum_{i=1}^3 b_i \equiv n \pmod{p}}} \prod_{i=1}^3 \frac{\mathcal{A}_{a_i}(b_i \bmod p)}{\mathcal{A}_{a_i}}. \end{aligned}$$

Since  $p \nmid \Delta_1 \Delta_2 \Delta_3$ , we see that  $\mathcal{A}_{a_i}(b_i \bmod p) / \mathcal{A}_{a_i} = \delta_{a_i}(b_i \bmod d) / \mathcal{L}_{a_i}$ .

Using (4.6), multiplicativity and Lemma 4.4, we infer that

$$S_{\mathbf{a},1}(n) = \prod_{p \nmid \Delta_1 \Delta_2 \Delta_3} \left( 1 + \sum_{c \in (\mathbb{Z}/p\mathbb{Z})^*} e_p(-nc) \prod_{i=1}^3 \mathcal{M}_{a_i}(c, p) \right) = \prod_{p \nmid \Delta_1 \Delta_2 \Delta_3} \sigma_{\mathbf{a},n}(p). \tag{4.7}$$

We now turn our attention to  $S_{\mathbf{a},0}(n)$ . Letting  $d_{\mathbf{w}} := \Delta_{\mathbf{w}}/q(\mathbf{w})$  we use Lemma 4.3 to obtain

$$\begin{aligned} S_{\mathbf{a},0}(n) &= \sum_{\substack{(d_{\mathbf{w}})_{\mathbf{w} \neq (1,1,1)} \in \mathbb{N}^7 \\ d_{\mathbf{w}} | \Delta_{\mathbf{w}}}} \sum_{(c^{[\mathbf{w}]}) \in \prod_{\mathbf{w} \neq (1,1,1)} \left( \frac{\mathbb{Z}}{(\Delta_{\mathbf{w}}/d_{\mathbf{w}})\mathbb{Z}} \right)^*} \left( \prod_{\mathbf{w} \neq (1,1,1)} e\left(-nc^{[\mathbf{w}]}d_{\mathbf{w}}/\Delta_{\mathbf{w}}\right) \right) \\ &\quad \times \prod_{i=1}^3 \left\{ \mathcal{D}_{a_i}((c^{[\mathbf{w}]}d_{\mathbf{w}})_{\mathbf{w}(i)=0}, (\Delta_{\mathbf{w}})_{\mathbf{w}(i)=0}) \prod_{\substack{\mathbf{w}(i)=1 \\ \mathbf{w} \neq (1,1,1)}} \mathcal{M}_{a_i}(c^{[\mathbf{w}]}d_{\mathbf{w}}, \Delta_{\mathbf{w}}) \right\}. \end{aligned}$$

For any  $d_w$  with  $d_w \mid \Delta_w$  the elements  $y^{[w]} \pmod{\Delta_w}$  that satisfy the condition  $\gcd(y^{[w]}, \Delta_w) = d_w$  are exactly those of the form

$$y^{[w]} = c^{[w]}d_w, \quad c^{[w]} \in \left(\frac{\mathbb{Z}}{(\Delta_w/d_w)\mathbb{Z}}\right)^*.$$

We thus obtain that the sum over  $d_w, c^{[w]}$  equals

$$\sum_{(y^{[w]}) \in \prod_{w \neq (1,1,1)} (\mathbb{Z}/\Delta_w\mathbb{Z})} \left( \prod_{w \neq (1,1,1)} e\left(-ny^{[w]}/\Delta_w\right) \right) \times \prod_{i=1}^3 \left\{ \mathcal{D}_{a_i}((y^{[w]})_{w(i)=0}, (\Delta_w)_{w(i)=0}) \prod_{\substack{w(i)=1 \\ w \neq (1,1,1)}} \mathcal{M}_{a_i}(y^{[w]}, \Delta_w) \right\}.$$

By definition,  $\Delta_{(1,1,1)} = 1$ , so  $\mathfrak{D}_a = \prod_{w \neq (1,1,1)} \Delta_w$ . Note that  $\gcd(\Delta_w, \Delta_v) = 1$  for  $w \neq v$ . Using the Chinese remainder theorem and writing every  $y \pmod{\prod_{v \neq (1,1,1)} \Delta_v}$  as

$$y = \sum_{w \neq (1,1,1)} y^{[w]} \prod_{v \notin \{w, (1,1,1)\}} \Delta_v,$$

we see that the sum over  $y^{[w]}$  equals

$$\sum_{y \pmod{\mathfrak{D}_a}} e(-ny/\mathfrak{D}_a) \prod_{i=1}^3 \left( \sum_{b_i \pmod{\mathfrak{D}_a}} e(b_i y/\mathfrak{D}_a) \delta_{a_i}(b_i \pmod{\mathfrak{D}_a}) \right).$$

This equals clearly

$$\mathfrak{D}_a \sum_{\substack{\mathbf{b} \pmod{\mathfrak{D}_a} \\ \sum_{i=1}^3 b_i \equiv n \pmod{\mathfrak{D}_a}}} \prod_{i=1}^3 \delta_{a_i}(b_i \pmod{\mathfrak{D}_a}),$$

thus, recalling (1.12), we have shown that

$$S_{\mathbf{a},0}(n) = \sigma_{\mathbf{a},n}(\mathfrak{D}_a) \prod_{i=1}^3 \mathcal{L}_{a_i}. \tag{4.8}$$

The proof of (1.14) is concluded upon combining (4.5), (4.7) and (4.8).

#### 4.2. The proof of (1.15)

We begin by finding an explicit expression for  $\sigma_{\mathbf{a},n}(p)$ , for  $p \nmid \Delta_1 \Delta_2 \Delta_3$ , that is explicit in terms of  $n$  and the  $h_{a_i}$ . Define

$$\theta_a(p) := \begin{cases} 1, & \text{if } p \mid h_a, \\ \frac{1}{p}, & \text{if } p \nmid h_a. \end{cases}$$

LEMMA 4.5. For an integer  $c$  and a prime  $p$  with  $p \nmid c$  we have

$$\mathcal{M}_a(c, p) = -\frac{(1 + \theta_a(p)e_p(c))}{(p - 1 - \theta_a(p))}.$$

*Proof.* Combining (1.6) and (4.4) we immediately infer

$$\mathcal{M}_a(c, p) = \frac{1}{(p-1-\theta_a(p))} \sum_{\substack{b \pmod p \\ \gcd(b,p)=1 \\ \gcd(b-1,p,h_a)=1}} e_p(bc) \prod_{\substack{\ell \text{ prime} \\ \ell \mid \gcd(b-1,p)}} \left(1 - \frac{1}{\ell}\right).$$

It is now easy to see that the sum over  $b$  equals  $-1 - e_p(c)$  or  $-1 - e_p(c)/p$  according to whether  $p \mid h_a$  or  $p \nmid h_a$ .

Let us denote the elementary symmetric polynomials in  $\theta_{a_i}(p)$  by

$$\begin{aligned} \Xi_0(p) &:= 1, \\ \Xi_1(p) &:= \theta_{a_1}(p) + \theta_{a_2}(p) + \theta_{a_3}(p), \\ \Xi_2(p) &:= \theta_{a_1}(p)\theta_{a_2}(p) + \theta_{a_2}(p)\theta_{a_3}(p) + \theta_{a_1}(p)\theta_{a_3}(p), \\ \Xi_3(p) &:= \theta_{a_1}(p)\theta_{a_2}(p)\theta_{a_3}(p). \end{aligned}$$

LEMMA 4.6. *For every odd integer  $n$  and prime  $p \nmid \prod_{i=1}^3 \Delta_i$  we have*

$$\sigma_{\mathbf{a},n}(p) = 1 - \frac{p}{\prod_{1 \leq i \leq 3} (p-1-\theta_{a_i}(p))} \left( \sum_{\substack{0 \leq j \leq 3 \\ j \equiv n \pmod p}} \Xi_j(p) \right) + \prod_{1 \leq i \leq 3} \left( \frac{1 + \theta_{a_i}(p)}{p-1-\theta_{a_i}(p)} \right).$$

*Proof.* By Lemma 4.4 and Lemma 4.5 we see that

$$\sigma_{\mathbf{a},n}(p) = 1 - \frac{1}{\prod_{1 \leq i \leq 3} (p-1-\theta_{a_i}(p))} \sum_{c \in (\mathbb{Z}/p\mathbb{Z})^*} e_p(-cn) \prod_{1 \leq i \leq 3} (1 + \theta_{a_i}(p)e_p(c)).$$

The sum over  $c$  equals

$$\sum_{0 \leq j \leq 3} \Xi_j(p) \sum_{c \in (\mathbb{Z}/p\mathbb{Z})^*} e_p(c(j-n)) = p \left( \sum_{\substack{0 \leq j \leq 3 \\ j \equiv n \pmod p}} \Xi_j(p) \right) - \prod_{1 \leq i \leq 3} (1 + \theta_{a_i}(p))$$

and the proof is complete.

LEMMA 4.7. *Let  $n$  be an odd integer. If  $3 \mid \Delta_1 \Delta_2 \Delta_3$ , then  $\prod_{p \nmid \Delta_1 \Delta_2 \Delta_3} \sigma_{\mathbf{a},n}(p) \neq 0$ . If  $3 \nmid \Delta_1 \Delta_2 \Delta_3$ , then the following are equivalent:*

- (1)  $\prod_{p \nmid \Delta_1 \Delta_2 \Delta_3} \sigma_{\mathbf{a},n}(p) = 0$ ;
- (2)  $\sigma_{\mathbf{a},n}(3) = 0$ ;
- (3) *one of the following two conditions holds:*

- 3 divides every element in the set  $\{h_{a_1}, h_{a_2}, h_{a_3}\}$  and  $3 \nmid n$ ; or*
- 3 divides exactly two elements in the set  $\{h_{a_1}, h_{a_2}, h_{a_3}\}$ , and  $n \equiv 1 \pmod 3$ .*

Furthermore,  $\prod_{p \nmid \Delta_1 \Delta_2 \Delta_3} \sigma_{\mathbf{a},n}(p) \neq 0$  implies  $\prod_{p \nmid \Delta_1 \Delta_2 \Delta_3} \sigma_{\mathbf{a},n}(p) \gg 1$ , with an absolute implied constant.

*Proof.* For a prime  $p \nmid \Delta_1 \Delta_2 \Delta_3$  with  $p \geq 5$  there exists at most one  $0 \leq j \leq 3$  satisfying  $j \equiv n \pmod{p}$ , therefore

$$\sum_{\substack{0 \leq j \leq 3 \\ j \equiv n \pmod{p}}} \Xi_j(p) \leq 3.$$

Invoking Lemma 4.6 we obtain

$$\sigma_{\mathbf{a},n}(p) > 1 - \frac{3p}{(p-2)^3} + \frac{1}{(p-1)^3}.$$

Since by assumption no  $a_i$  is a square, we have  $2 \nmid h_{a_1} h_{a_2} h_{a_3}$ . The fact that  $n$  is odd implies that

$$\sum_{\substack{0 \leq j \leq 3 \\ j \equiv n \pmod{2}}} \Xi_j(2) = \Xi_1(2) + \Xi_3(2) = \frac{13}{8},$$

hence if  $\Delta_1 \Delta_2 \Delta_3$  is odd we can use Lemma 4.6 to show that  $\sigma_{\mathbf{a},n}(2) = 2$ . We have shown that for odd  $n$  one has

$$\prod_{\substack{p \nmid \Delta_1 \Delta_2 \Delta_3 \\ p \neq 3}} \sigma_{\mathbf{a},n}(p) \gg 1$$

with an absolute implied constant and it remains to study  $\sigma_{\mathbf{a},n}(3)$ . One can find an explicit formula for this density by fixing the congruence class of  $n \pmod{3}$ . For example, if  $n \equiv 1 \pmod{3}$  we have

$$\sigma_{\mathbf{a},n}(3) = 1 - \frac{3(\theta_{a_1}(3) + \theta_{a_2}(3) + \theta_{a_3}(3))}{\prod_{1 \leq i \leq 3} (2 - \theta_{a_i}(3))} + \prod_{1 \leq i \leq 3} \left( \frac{1 + \theta_{a_i}(3)}{2 - \theta_{a_i}(3)} \right)$$

and we can check that  $\sigma_{\mathbf{a},n}(3) = 0$  if and only if at most one of the  $\theta_i$  is equal to  $1/3$ . A case by case analysis reveals that if  $n \equiv 2 \pmod{3}$  then  $\sigma_{\mathbf{a},n}(3) = 0$  if and only if  $(\theta_{a_i}(3))_i = (1, 1, 1)$  and that if  $n \equiv 0 \pmod{3}$  then  $\sigma_{\mathbf{a},n}(3)$  never vanishes. Noting that  $\sigma_{\mathbf{a},n}(3)$  attains only finitely many values as it only depends on  $n \pmod{3}$  and the choice of  $(\theta_{a_i}(3))_i \in \{1, 1/3\}^3$ , we see that there exists an absolute constant  $c$  such that if  $\sigma_{\mathbf{a},n}(3) > 0$  then  $\sigma_{\mathbf{a},n}(3) > c$ , thus concluding our proof.

We next provide a lower bound for  $S_{\mathbf{a},0}(n)$ , see (4.8). One could proceed by finding explicit expressions, however, this will lead to rather more complicated formulas than the one for  $S_{\mathbf{a},1}(n)$  in Lemma 4.6. We shall instead opt to bound the densities  $\delta_a(b_i \pmod{\mathfrak{D}_a})$  from below in (4.8) and then count the number of solutions of the equation  $n \equiv x_1 + x_2 + x_3 \pmod{\mathfrak{D}_a}$  such that for every  $i$  we have  $\delta_a(x_i \pmod{\mathfrak{D}_a}) \neq 0$ .

LEMMA 4.8. *Given any integers  $q$  and  $x$  such that  $q$  is positive and  $\delta_a(x \pmod{q}) > 0$ , we have*

$$\delta_a(x \pmod{q}) \gg \frac{\varphi(h_a)}{qh_a},$$

*with an absolute implied constant.*

*Proof.* Under the assumptions of our lemma we have the following due to Definition 1.4,

$$\begin{aligned} \delta_a(x \bmod q) \mathcal{A}_a^{-1} \frac{\varphi(q)}{f_a^\dagger(q)} \prod_{p|x-1, p|q} \left(1 - \frac{1}{p}\right)^{-1} \\ = 1 + \mu \left( \frac{2|\Delta_a|}{\gcd(q, \Delta_a)} \right) \left( \frac{\beta_a(q)}{x} \right) f_a^\ddagger \left( \frac{|\Delta_a|}{\gcd(q, \Delta_a)} \right). \end{aligned}$$

The right-hand side is either  $\geq 1$  or equal to  $1 - f_a^\ddagger(|\Delta_a| \gcd(q, \Delta_a)^{-1})$ . In the latter case, since the right-hand side must be positive and  $f_a^\ddagger(|\Delta_a| \gcd(q, \Delta_a)^{-1})^{-1}$  is an integer, we see that the right-hand side is  $\geq 1/2$ . Therefore, under the assumptions of our lemma we have

$$\delta_a(x \bmod q) \geq \frac{\mathcal{A}_a f_a^\dagger(q)}{2 \varphi(q)} \prod_{p|x-1, p|q} \left(1 - \frac{1}{p}\right).$$

It is obvious that  $\mathcal{A}_a f_a^\dagger(q) \gg \varphi(h_a)/h_a$ , with an implied absolute constant. This is sufficient for our lemma owing to  $\prod_{p|x-1, p|q} (1 - 1/p) \geq \varphi(q)/q$ .

Recalling (1.12) we see that

$$\sigma_{a,n}(\mathfrak{D}_a) \prod_{i=1}^3 \mathcal{L}_{a_i} = \mathfrak{D}_a \sum_{\substack{b_1, b_2, b_3 \pmod{\mathfrak{D}_a} \\ b_1 + b_2 + b_3 \equiv n \pmod{\mathfrak{D}_a}}} \prod_{i=1}^3 \delta_{a_i}(b_i \bmod \mathfrak{D}_a),$$

thus, if  $\sigma_{a,n}(\mathfrak{D}_a) > 0$  then there exist  $x_1, x_2, x_3 \pmod{\mathfrak{D}_a}$  such that  $\prod_{i=1}^3 \delta_{a_i}(x_i \bmod \mathfrak{D}_a) > 0$  and  $x_1 + x_2 + x_3 \equiv n \pmod{\mathfrak{D}_a}$ . Invoking Lemma 4.8 we see that if  $\sigma_{a,n}(\mathfrak{D}_a) > 0$  then

$$\sigma_{a,n}(\mathfrak{D}_a) \prod_{i=1}^3 \mathcal{L}_{a_i} \geq \mathfrak{D}_a \prod_{i=1}^3 \delta_{a_i}(x_i \bmod \mathfrak{D}_a) \gg \mathfrak{D}_a^{-2} \prod_{i=1}^3 \frac{\varphi(h_{a_i})}{h_{a_i}}.$$

Recalling (1.13) we obtain  $\mathfrak{D}_a \leq [\Delta_1, \Delta_2, \Delta_3] \leq |\Delta_1 \Delta_2 \Delta_3|$ , hence

$$\sigma_{a,n}(\mathfrak{D}_a) \prod_{i=1}^3 \mathcal{L}_{a_i} \gg \prod_{i=1}^3 \frac{\varphi(h_{a_i})}{|\Delta_i|^2 h_{a_i}},$$

with an absolute implied constant. Combined with Lemma 4.7, this concludes the proof of (1.15).

### 4.3. The proof of Theorem 1.5

The theorem consists of two assertions, (1.14) and (1.15). The former was proved in Section 4.1 and the latter in Section 4.2.

### 4.4. The proof of Corollary 1.6

Obviously, (1) implies (2). For the reverse direction, let  $d \in \{3, \mathfrak{D}_a\}$  and let  $p_1, p_2, p_3$  be primes not dividing  $2d$ , such that each  $a_i$  is a primitive root modulo  $p_i$  and  $p_1 + p_2 + p_3 \equiv n \pmod{d}$ . Thus, for every  $i = 1, 2, 3$  the progression  $p_i \pmod{d}$  satisfies  $\gcd(p_i, d) = 1$  and contains an odd prime having  $a_i$  as a primitive root. We can now use the following observation due to Lenstra [10, p.216]: if  $\gcd(x, d) = 1$  and  $\delta_a(x \bmod d) = 0$ , then either there is no prime  $p \equiv x \pmod{d}$  with  $\mathbb{F}_p^* = \langle a \rangle$ , or there is one such prime, which must be equal to 2. This shows that we must have  $\delta_a(x_i \bmod d) > 0$  for every  $i = 1, 2, 3$ . Using the fact that



$x_1 + x_2 + x_3 \equiv n \pmod{d}$ , as well as Definition (1.12) shows that  $\sigma_{\mathfrak{a},n}(\mathfrak{D}_{\mathfrak{a}})\sigma_{\mathfrak{a},n}(3) > 0$ . By Lemma 4.7, we get  $\mathcal{A}_{\mathfrak{a}}(n) > 0$ , and thus  $\mathcal{A}_{\mathfrak{a}}(n) \gg 1$  by (1.15). Thus, (1) follows immediately from Theorem 1.1 and the trivial estimate

$$\sum_{\substack{p_1+p_2+p_3=n \\ \exists i: p_i \nmid 6\Delta_1\Delta_2\Delta_3}} \left( \prod_{i=1}^3 \log p_i \right) \ll n(\log n)^3.$$

4.5. The proof of Theorem 1.7

First note that  $\mathfrak{D}_{(a,a,a)} = |\Delta_a|$ . It is clear that for the proof of Theorem 1.7 we need to find equivalent conditions for  $n$  to satisfy

$$\sigma_{(a,a,a),n}(|\Delta_a|) \prod_{p \nmid \Delta_a} \sigma_{(a,a,a),n}(p) > 0.$$

By Lemma 4.7 the condition  $\prod_{p \nmid \Delta_a} \sigma_{(a,a,a),n}(p) \neq 0$  is equivalent to

$$\begin{cases} n \equiv 3 \pmod{6}, & \text{if } 3 \mid h_a \text{ and } 3 \nmid \Delta_a, \\ n \equiv 1 \pmod{2}, & \text{otherwise.} \end{cases} \tag{4.9}$$

Hence it remains to find equivalent conditions for  $n$  to satisfy  $\sigma_{(a,a,a),n}(|\Delta_a|) > 0$ .

PROPOSITION 4.9. Assume that  $n$  is an odd positive integer.

- (1) If  $3 \nmid \gcd(\Delta_a, h_a)$  or  $3 \mid n$ , and if  $\Delta_a$  has a prime divisor that is greater than 7, then  $\sigma_{(a,a,a),n}(|\Delta_a|) > 0$ .
- (2) If  $3 \mid \gcd(\Delta_a, h_a)$  and  $3 \nmid n$ , then  $\sigma_{(a,a,a),n}(|\Delta_a|) = 0$ .

*Proof.* It can be seen directly from Definition 1.4 that the quantity  $\delta_a(x_i \pmod{|\Delta_a|})$  is non-zero if and only if

$$\gcd(x_i - 1, \Delta_a, h_a) = 1, \quad \gcd(x_i, \Delta_a) = 1 \text{ and } \left( \frac{\Delta_a}{x_i} \right) = -1. \tag{4.10}$$

In view of Definition 1.12, we need to find conditions under which there are  $x_1, x_2, x_3 \in \mathbb{Z}$  with  $x_1 + x_2 + x_3 \equiv n \pmod{\Delta_a}$ , such that each  $x_i$  satisfies (4.10).

To prove (2), we observe that the first two conditions in (4.10) imply that  $x_i \equiv 2 \pmod{3}$ , hence  $3 \mid n$ .

Let us now prove (1). Write  $\Delta_a = \prod_{p \mid \Delta_a} D_p$ , where  $D_2 \in \{-8, -4, 8\}$  and  $D_p = (-1)^{(p-1)/2} p$  for  $p \geq 3$ . Let  $p' > 7$  be the largest prime divisor of  $\Delta_a$ . For every  $p < p'$ , we find  $x_1^{(p)}, x_2^{(p)}, x_3^{(p)} \pmod{D_p}$  that solve the congruence  $x_1^{(p)} + x_2^{(p)} + x_3^{(p)} \equiv n \pmod{D_p}$  and satisfy  $\gcd(x_i^{(p)} - 1, \Delta_a, h_a) = \gcd(x_i^{(p)}, \Delta_a) = 1$ . If  $p > 3$ , this is possible for every  $n$  by a simple application of the Cauchy–Davenport Theorem. If  $p = 3$ , it is possible precisely by our assumption that then  $3 \nmid h_a$  or  $3 \mid n$ . Finally, for  $p = 2$ , it is possible since  $2 \nmid nh_a$ .

Let us now define  $x_i^{(p')}$ . Consider the sets

$$R := \left\{ x \in \mathbb{Z}/p'\mathbb{Z} : \left( \frac{x}{p'} \right) = 1, x \not\equiv 1 \pmod{p'} \right\}, \quad N := \left\{ x \in \mathbb{Z}/p'\mathbb{Z} : \left( \frac{x}{p'} \right) = -1 \right\}.$$

If  $\prod_{\substack{p|\Delta_a \\ p < p'}} (D_p/x_i^{(p)}) = 1$ , we pick  $x_i^{(p')} \in N$ , and if  $\prod_{\substack{p|\Delta_a \\ p < p'}} (D_p/x_i^{(p)}) = -1$ , we pick  $x_i^{(p')} \in R$ . We can always do so and achieve  $x_1^{(p')} + x_2^{(p')} + x_3^{(p')} \equiv n \pmod{p'}$ , as the sets

$$R + R + R, \quad R + R + N, \quad R + N + N, \quad N + N + N$$

cover all of  $\mathbb{Z}/p'\mathbb{Z}$ . This follows from a direct computation if  $p' = 11$  and from the Cauchy–Davenport Theorem if  $p' \geq 13$ .

To finish our proof of (1), we pick integers  $x_i$  that satisfy  $x_i \equiv x_i^{(p')} \pmod{D_p}$  for all  $p \mid \Delta_a$ . Then quadratic reciprocity ensures that

$$\left(\frac{\Delta_a}{x_i}\right) = \left(\frac{x_i^{(p')}}{p'}\right) \prod_{\substack{p|\Delta_a \\ p < p'}} \left(\frac{D_p}{x_i^{(p')}}\right) = -1$$

for all  $i$ . Hence, the  $x_i$  satisfy (4.10), and moreover  $x_1 + x_2 + x_3 \equiv n \pmod{\Delta_a}$ .

*Proof of Theorem 1.7.* First let us note that the fundamental discriminants with every prime smaller than 11 are of the form

$$D_2^{i_1} (-3)^{i_2} 5^{i_3} (-7)^{i_4},$$

where  $D_2$  is an integer in the set  $\{-4, 8, -8\}$  and every exponent  $i_j$  is either 0 or 1. This gives a finite set of values for  $\Delta_a$  and it is straightforward to use a computer program that finds all congruence classes  $n \pmod{\Delta_a}$  such that  $n \equiv x_1 + x_2 + x_3 \pmod{\Delta_a}$  for some  $\mathbf{x} \in (\mathbb{Z}/\Delta_a\mathbb{Z})^3$  satisfying all of the conditions (4.10) for  $1 \leq i \leq 3$ .

By Definition 1.4 these conditions are equivalent to  $\delta_a(x_i \pmod{|\Delta_a|}) \neq 0$  and when combined with (4.9) they provide the congruence classes for  $n$  in every row of the table in Theorem 1.7 apart from the last two rows.

For the last two rows,  $\Delta_a$  has a prime factor greater than 7. In this case, if  $3 \mid h_a$ , then (4.9) and Proposition 4.9 yield the condition  $n \equiv 3 \pmod{6}$ . If, on the other hand,  $3 \nmid h_a$  then we get no further condition apart from  $n$  odd.

#### 4.6. Non-factorisation of $\mathcal{A}_a(n)$

We finish by showing that the right-hand side in (1.14) does not always factorise as an Euler product of a specific form. Namely, assume that for every non-square integer  $a \neq -1$  we are given a sequence of real numbers  $\lambda_a : \mathbb{Z}^2 \rightarrow [0, \infty)$  such that for every prime  $p$  and integers  $x, x'$  we have

$$\delta_a(x \pmod{p}) > 0 \implies \lambda_a(x, p) > 0 \tag{4.11}$$

and

$$x \equiv x' \pmod{p} \implies \lambda_a(x, p) = \lambda_a(x', p).$$

Now, in parallel with (1.12), let us define

$$\varpi_{p,a}(n) := \left( \sum_{\substack{b_1, b_2, b_3 \pmod{p} \\ b_1 + b_2 + b_3 \equiv n \pmod{p}}} \prod_{i=1}^3 \lambda_a(x, p) \right) \left( \sum_{\substack{b_1, b_2, b_3 \pmod{p} \\ b_1 + b_2 + b_3 \equiv n \pmod{p}}} \frac{1}{p^3} \right)^{-1}.$$

The fact that the quantities  $\varpi_{p,a}(n)$  are well-defined follows from the periodicity of  $\lambda_a$ .

We will see that one cannot have the following factorisation for all odd integers  $n$ ,

$$\mathcal{L}_a^3 \sigma_{(a,a,a),n}(|\Delta_a|) = \prod_{p|\Delta_a} \varpi_{p,a}(n). \tag{4.12}$$

Indeed, if  $a := (-15)^5 = -759375$  then by Definition 1.4 we easily see that

$$\delta_{-759375}(x \bmod 15) > 0 \Leftrightarrow x \bmod 15 \in \{7, 13, 14 \pmod{15}\},$$

hence for all integers  $n \equiv 7 \pmod{15}$  we have  $\sigma_{(a,a,a),n}(|\Delta_a|) = 0$  due to (1.12) and the fact that for all  $\mathbf{x} \in \{7, 13, 14\}^3$  one has  $\sum_{i=1}^3 x_i \not\equiv 7 \pmod{15}$ . Definition 1.4 furthermore implies that

$$\delta_{-759375}(x \bmod 3) > 0 \iff x \bmod 3 \in \{1, 2 \pmod{3}\}$$

and

$$\delta_{-759375}(y \bmod 5) > 0 \iff y \bmod 5 \in \{2, 3, 4 \pmod{5}\},$$

therefore whenever  $n \equiv 7 \pmod{15}$  then the vectors  $\mathbf{x} = (1, 1, 2)$  and  $\mathbf{y} = (4, 4, 4)$  satisfy

$$\sum_{i=1}^3 x_i \equiv n \pmod{3}, \sum_{i=1}^3 y_i \equiv n \pmod{5} \text{ and } \prod_{i=1}^3 \delta_{-759375}(x_i \bmod 3) \delta_{-759375}(y_i \bmod 5) > 0.$$

By (4.11) this implies that  $\varpi_{3,-759375}(n) > 0$ ,  $\varpi_{5,-759375}(n) > 0$ , which contradicts (4.12) due to  $\sigma_{(a,a,a),n}(|\Delta_a|) = 0$ .

*Acknowledgements.* This work was completed while Christopher Frei and Peter Koymans were visiting the Max Planck Institute in Bonn, the hospitality of which is greatly acknowledged.

#### REFERENCES

- [1] H. COHEN. *Number Theory. Vol. I. Tools and Diophantine Equations* (Springer, New York, 2007).
- [2] R. GUPTA and R. MURTY. A remark on Artin's conjecture. *Invent. Math.* **78** (1984), 127–130.
- [3] H. HALBERSTAM and H.-E. RICHERT. *Sieve methods*. London Mathematical Society Monographs (Academic Press Providence, RI, 1974).
- [4] G. H. HARDY and J. E. LITTLEWOOD. Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes. *Acta Math.* **44** (1923), 1–70.
- [5] D. R. HEATH-BROWN. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford Ser. (2)* **37** (1986), 27–38.
- [6] A. H. HELFGOTT. The ternary Goldbach problem. arXiv:0903.4503, (2015).
- [7] C. HOOLEY. On Artin's conjecture. *J. Reine Angew. Math.* **225** (1967), 209–220.
- [8] H. IWANIEC and E. KOWALSKI. *Analytic number theory*. American Math. Soc. (Providence, RI, 2004).
- [9] D. M. KANE. An asymptotic for the number of solutions to linear equations in prime numbers from specified Chebotarev classes. *Int. J. Number Theory* **9** (2013), 1073–1111.
- [10] H. W. LENSTRA. On Artin's conjecture and Euclid's algorithm in global fields. *Invent. Math.* **42** (1977), 201–224.
- [11] H. W. LENSTRA, P. STEVENHAGEN and P. MOREE. Character sums for primitive root densities. *Math. Proc. Camb. Phil. Soc.* **157** (2014), 489–511.
- [12] P. MOREE. On primes in arithmetic progression having a prescribed primitive root. II. *Funct. Approx. Comment. Math.* **39** (2008), 133–144.
- [13] P. MOREE. Artin's primitive root conjecture—a survey. *Integers* **12** (2012), 1305–1416.
- [14] J.-P. SERRE. Résumé des cours de 1977–1978. *Annuaire du Collège de France* (1978), 67–70.

- [15] X. SHAO. A density version of the Vinogradov three primes theorem. *Duke Math. J.* **163** (2014), 489–512.
- [16] P. STEVENHAGEN. The correction factor in Artin's primitive root conjecture. *J. Théor. Nombres Bordeaux* **15** (2003), 383–391.
- [17] I. M. VINOGRADOV. Representation of an odd number as a sum of three primes. *C. R. (Dokl.) Acad. Sci. URSS, n. Ser.* **15** (1937), 169–172.