Diophantine equations in positive characteristic

Koymans, P.H.

Chapter 7

Vinogradov's three primes theorem with primes having given primitive roots

Joint work with Christopher Frei and Efthymios Sofos

Abstract

The first purpose of this chapter 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.

7.1 Introduction

Can we represent an odd integer as a sum of 3 odd primes all of which have 27 as a primitive root? Lenstra [51] was the first to address the problem of primes with a fixed primitive root and lying in an arithmetic progression. One of his results [51, Th.(8.3)] states that if $b \neq 5 \pmod{12}$ 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 chapter, 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 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 [30] towards ternary Goldbach with Hooley's [35] conditional proof of Artin's conjecture.

Theorem 7.1.1. *Let* $\mathbf{a} = (a_1, a_2, a_3) \in \mathbb{Z}^3$ *such that no* a_i *is* -1 *or a perfect square. Assuming* HRH(a_i) *for* $i = 1, 2, 3$*, we have*

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i:\ \mathbb{F}_{p_i}^* = \langle a_i \rangle}} \prod_{i=1}^{3} \log p_i = \mathcal{A}_{\mathbf{a}}(n) n^2 + o(n^2), \qquad \text{as} \qquad n \to +\infty, \tag{7.1}$$

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 bulk of this chapter will be 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 7.1.1 as a local-global principle and gives the following as a simple consequence.

Corollary 7.1.2. *Assume* 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* $n \equiv 3 \bmod 12$.

We can also get an explicit saving in the error term, for the price of working under a stronger generalised Riemann hypothesis. Let 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 7.1.3. *Let* a_1, a_2, a_3 *be three integers none of which is* -1 *or a perfect square. Assuming* HRH'(a_i) *for* $i = 1, 2, 3$*, we have for* $\beta \in (0, 1)$*,*

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i:\ \mathbb{F}_{p_i}^* = \langle a_i \rangle}} \prod_{i=1}^{3} \log p_i = \mathcal{A}_{\mathbf{a}}(n) n^2 + O_{\mathbf{a},\beta}(n^2 (\log n)^{-\beta}), \tag{7.2}$$

where the implied constant is effective and depends at most on a_1, a_2, a_3 *and* β.

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.

7.1.1 Artin's conjecture

Fix an integer $a \neq -1$ which is not a perfect square. A question going back to Gauss regards the infinitude of primes having a as a primitive root. It was realised by Artin that the question admits an interpretation through algebraic number theory. Denote by ζ_k a primitive kth root of unity and define for any positive square-free integer k the number field

$$G_{a,k} := \mathbb{Q}(a^{1/k}, \zeta_k). \tag{7.3}$$

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 a collective effort due to Artin, Lehmer and Heilbronn. Define

$$\Delta_a := \mathrm{Disc}(\mathbb{Q}(\sqrt{a})), \text{ the discriminant of } \mathbb{Q}(\sqrt{a}) \tag{7.4}$$

$$h_a := \max\big\{m \in \mathbb{N} : a \text{ is an } m\text{th power}\big\}, \tag{7.5}$$

$$\mathcal{A}_a := \prod_{p \mid h_a} \left(1 - \frac{1}{p-1}\right) \prod_{p \nmid h_a} \left(1 - \frac{1}{p(p-1)}\right) \tag{7.6}$$

and for positive integers q let

$$f_a^{\ddagger}(q) := \Big(\prod_{p \mid q, p \mid h_a} (p-2)^{-1} \Big) \Big(\prod_{p \mid q, p \nmid h_a} (p^2 - p - 1)^{-1} \Big). \tag{7.7}$$

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

$$\mathcal{L}_a := \mathcal{A}_a \cdot \big(1 + \mu(2|\Delta_a|) f_a^{\ddagger}(|\Delta_a|)\big), \tag{7.8}$$

where μ is the Möbius function. Artin's conjecture then states that

$$\lim_{x \to +\infty} \frac{\#\big\{p \leq x : \mathbb{F}_p^* = \langle a \rangle\big\}}{\#\{p \leq x\}} = \mathcal{L}_a. \tag{7.9}$$

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 [35]. His method is pivotal in the present work. Notable progress was later made by Heath-Brown [32], who building on work of Gupta and Murty [28], 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 [60]. Lenstra [51] used Hooley's method to show, conditionally on HRH(a), the existence of the Dirichlet density of primes in an arithmetic progression and with a as primitive root. An explicit formula

for these densities was given later by Moree [59]. To describe Moree's result we need the following notation. Let

$$\beta_a(q) := \begin{cases} (-1)^{\frac{\frac{\Delta_a}{\gcd(q,\Delta_a)}-1}{2}} \gcd(q,\Delta_a), & \text{if } \frac{\Delta_a}{\gcd(q,\Delta_a)} \equiv 1 \,(\mathrm{mod}\ 2) \\ 1 & \text{otherwise,} \end{cases} \tag{7.10}$$

and observe that $\beta_a(q)$ is a fundamental discriminant in case $\Delta_a/\gcd(q,\Delta_a) \equiv 1 \bmod 2$. For positive integers q let

$$f_a^{\dagger}(q) := \prod_{p|h_a, p|q} \left(1 - \frac{1}{p-1}\right)^{-1} \prod_{p\nmid h_a, p|q} \left(1 - \frac{1}{p(p-1)}\right)^{-1}. \tag{7.11}$$

Definition 7.1.4. Assume that $a \neq -1$ is a non-square integer, let Δ_a, h_a be as in (7.4), (7.5) and assume that x, q are integers with $q > 0$. We define

$$\mathcal{A}_a(x \bmod q) := \mathcal{A}_a \cdot \begin{cases} \frac{f_a^{\dagger}(q)}{\phi(q)} \prod_{p|x-1, p|q} \left(1 - \frac{1}{p}\right), & \text{if } \gcd(x-1, q, h_a) = \gcd(x,q) = 1, \\ 0, & \text{otherwise,} \end{cases} \tag{7.12}$$

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 $\phi(\cdot)$ is the Euler totient function and $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker quadratic symbol.

Moree's result [59] states that, conditionally under HRH(a), the Dirichlet 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.

7.1.2 Ternary Goldbach problem

The ternary Goldbach problem has been one of the most central subjects in analytic number theory; it asserts that every odd integer greater than 5 is the sum of 3 primes. Hardy and Littlewood [30] 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 [74]. 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 β, and

$$\varrho_p(n) := p\Bigg(\sum_{\substack{b_1,b_2,b_3 \in (\mathbb{Z}/p\mathbb{Z})^* \\ b_1+b_2+b_3 \equiv n \pmod{p}}} \frac{1}{(p-1)^3} \Bigg). \tag{7.13}$$

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

$$p = \Bigg(\sum_{\substack{b_1,b_2,b_3 \pmod{p} \\ b_1+b_2+b_3 \equiv n \pmod{p}}} \frac{1}{p^3} \Bigg)^{-1}. \tag{7.14}$$

It should be mentioned that Helfgott [34] recently settled the ternary Goldbach problem. Using recent developments in additive combinatorics, Shao [65] 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 [65, Th.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 $\delta/\phi(q)$, 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 $\prod_{p\le T} p$ for some $T > 2$ then it is easy to see that

$$\delta_a(1 \bmod q)\phi(q) \le \prod_{p\le T} \Big(1 - \frac{1}{p}\Big) \ll \frac{1}{\log\log q}.$$

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 7.1.1. This approach would still require HRH(a_i) and besides the focal point of the chapter is the 'Artin factor' $\mathcal{A}_{\mathbf{a}}(n)$ in Theorem 7.1.1. A further result related to ours is that of Kane [38]. 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.

7.1.3 The factor $\mathcal{A}_{\mathbf{a}}(n)$

Let us now describe the representation of $\mathcal{A}_{\mathbf{a}}(n)$ that is obtained directly from the proof of Theorem 7.1.1. 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 $\gcd(b, q) = 1$, 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 $\mathrm{e}_q(z) := \exp(2\pi i z/q)$, for $z \in \mathbb{C}, q \in \mathbb{N}$. The exponential sum

$$S_{a,q,k}(z) := \sum_{b \in (\mathbb{Z}/q\mathbb{Z})^*} c_{a,q,k}(b)\mathrm{e}_q(zb) \tag{7.15}$$

and the entities

$$L_{\mathbf{a},q,\mathbf{k}}(z) := \prod_{i=1}^{3} S_{a_i,q,k_i}(z), \tag{7.16}$$

$$d_{\mathbf{a},\mathbf{k}}(q) := \prod_{i=1}^{3} [F_{a_i,q,k_i} : \mathbb{Q}] \tag{7.17}$$

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

$$\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n) := \sum_{q=1}^{\infty} \frac{1}{d_{\mathbf{a},\mathbf{k}}(q)} \sum_{\substack{z \in \mathbb{Z}/q\mathbb{Z} \\ \gcd(z,q)=1}} \mathrm{e}_q(-nz) L_{\mathbf{a},q,\mathbf{k}}(z). \tag{7.18}$$

It will be made clear in §7.2 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 7.3.2. With this notation in place, the leading factor in Theorem 7.1.1 and Theorem 7.1.3 is given by

$$\mathcal{A}_{\mathbf{a}}(n) = \frac{1}{2}\Bigg(\sum_{\mathbf{k} \in \mathbb{N}^3} \mu(k_1)\mu(k_2)\mu(k_3)\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n) \Bigg). \tag{7.19}$$

The sum over $\mathbf{k}$ will be shown to be absolutely convergent in Lemma 7.3.2. 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 [51], who studied the density of primes in arithmetic progressions and with a prescribed primitive root, as well as the work of Serre [64], 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

$$\sigma_{\mathbf{a},n}(d) := d\Bigg(\sum_{\substack{b_1,b_2,b_3 (\mathrm{mod}\ d) \\ b_1+b_2+b_3 \equiv n (\mathrm{mod}\ d)}} \prod_{i=1}^{3} \frac{\delta_{a_i}(b_i \bmod d)}{\mathcal{L}_{a_i}} \Bigg). \tag{7.20}$$

The factor d has an explanation that is identical to the explanation of the factor p in (7.13)-(7.14). Let $[\cdot]$ denote the least common multiple, $\nu_p(\cdot)$ be the p-adic valuation and define

$$\mathfrak{D}_{\mathbf{a}} := 2^{\min\{\nu_2(\Delta_{a_i}):1\le i\le 3\} - \max\{\nu_2(\Delta_{a_i}):1\le i\le 3\}} [\Delta_{a_1}, \Delta_{a_2}, \Delta_{a_3}]. \tag{7.21}$$

Theorem 7.1.5. *The factor $\mathcal{A}_{\mathbf{a}}(n)$ in Theorems 7.1.1 and 7.1.3 factorises as follows,*

$$\mathcal{A}_{\mathbf{a}}(n) = \frac{1}{2}\Big(\prod_{i=1}^{3} \mathcal{L}_{a_i}\Big)\sigma_{\mathbf{a},n}(\mathfrak{D}_{\mathbf{a}}) \prod_{p \nmid \mathfrak{D}_{\mathbf{a}}} \sigma_{\mathbf{a},n}(p). \tag{7.22}$$

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

$$\mathcal{A}_{\mathbf{a}}(n) \gg \prod_{i=1}^{3} \frac{\phi(h_{a_i})}{|\Delta_{a_i}|^2 h_{a_i}}, \tag{7.23}$$

with an absolute implied constant.

For an interpretation of the right side of (7.22) see §7.1.4. The proof of (7.22) (that will be provided in §7.4.1) requires adroit manoeuvring. This is because the densities $\delta_a(b_i \bmod d)$ in (7.20) 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 (7.22) does not factorise as an Euler product, see §7.4.6 for a precise statement of this phenomenon. The following consequence of Theorem 7.1.1 and Theorem 7.1.5 can be interpreted as a local-global principle.

Corollary 7.1.6. *Let a_1, a_2, a_3 be three integers none of which is -1 or a perfect square, and assume* $\mathrm{HRH}(a_i)$ *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 $d \in \{3, \mathfrak{D}_{\mathbf{a}}\}$, there are primes p_1, p_2, p_3 with $\gcd(p_1p_2p_3, 2d) = 1$ such that a_i is a primitive root for p_i for every $i = 1, 2, 3$ and $p_1 + p_2 + p_3 \equiv n \bmod d$.*

Though part *(2)* of Corollary 7.1.6 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 $\sigma_{\mathbf{a},d}(n) > 0$. In Lemma 7.4.7, we shall see that $\sigma_{\mathbf{a},n}(p) > 0$ whenever $p \nmid 3\Delta_{a_1}\Delta_{a_2}\Delta_{a_3}$. Moreover, it is clear from the definition in (7.20), that whether $\sigma_{\mathbf{a},d}(n) = 0$ or not is a local condition modulo d.

7.1.4 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 [64]. 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 and Lenstra–Stevenhagen–Moree [52], as well as the survey of Moree [60].

We now focus on the interpretation of the "Artin-factor" $\mathcal{A}_{\mathbf{a}}(n)$ with the help of (7.22). 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 (7.22) 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 (7.9).

The factors $\sigma_{\mathbf{a},n}(d)$ for $d \in \{\mathfrak{D}_{\mathbf{a}}\} \cup \{p \text{ prime } : p \nmid \mathfrak{D}_{\mathbf{a}}\}$ admit an explanation that is comparable to the analogous densities in the classical case of the ternary Goldbach problem, see (7.13). There is only one difference, namely that one has to use the weight

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

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 [52]), to provide a prediction for $\mathcal{A}_{\mathbf{a}}(n)$ with a method that is different to the one in §7.4.1.

7.1.5 The case where all primitive roots are equal

In our next theorem, we provide an explicit description of the local conditions in Corollary 7.1.6, 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 7.1.7. *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 one of the congruence conditions in the third row of the following table. The second to last row refers to all integers a not considered

in a row above it, as long as a is a third power. The last row refers to every integer a not considered in a row above it.

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

Theorem 7.1.7 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 7.1.2, whose proof we give now.

Proof of Corollary 7.1.2. If n is a sum of 3 odd primes all of which have primitive root 27, we saw in the first paragraph of this chapter that n must be $3 \bmod 12$. For the opposite direction we observe that if $a = 27$ then we have $\mathrm{Disc}(\mathbb{Q}(\sqrt{a})) = 12$ and $a \in \mathbb{Z}^3 \setminus (\{-1\} \cup \mathbb{Z}^2)$, hence alluding to the fifth row in the table of Theorem 7.1.7 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. □

7.1.6 Structure of the chapter

We study a generalisation of the ternary Goldbach problem in §7.2, where each of the three primes involved satisfies certain splitting conditions in a different number field

extension of $\mathbb{Q}$. The main result of §7.2 is Proposition 7.2.1, whose proof is given in §7.2.3.

Next, §7.3.1 contains the first steps for the combination of Hooley's argument [35] and the Hardy–Littlewood circle method. Theorem 7.1.1 will be proved in §7.3.2, while Theorem 7.1.3 is verified in §7.3.3.

The rest of our chapter, namely §7.4, deals with the 'Artin factor' $\mathcal{A}_{\mathbf{a}}(n)$. The former part of Theorem 7.1.1, viz. (7.22), is verified in §7.4.1, while the latter part, viz. (7.23), is established in §7.4.2. Corollary 7.1.6 and Theorem 7.1.7 are proved in §7.4.4 and §7.4.5 respectively. Finally, we show that $\mathcal{A}_{\mathbf{a}}(n)$ does not factorise as an Euler product in §7.4.6.

Notation 7.1.8. The letters p and ℓ 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

$$\mathrm{e}(z) := \exp(2\pi i z) \text{ and } \mathrm{e}_q(z) := \exp(2\pi i z/q), (z \in \mathbb{C}, q \in \mathbb{N}).$$

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.

7.2 Uniform ternary Goldbach with certain splitting conditions

In this section the letters k, k_i shall refer exclusively to positive square-free integers. Recall (7.3) and define

$$\mathrm{Spl}\,(G_{a,k}) := \{p \text{ prime in } \mathbb{N} : p \text{ splits completely in } G_{a,k}\}. \tag{7.24}$$

We study the asymptotics of the representation function

$$V_{\mathbf{a},\mathbf{k}}(n) := \sum_{\substack{p_1+p_2+p_3=n \\ \forall i:\ p_i \in \mathrm{Spl}\left(G_{a_i,k_i}\right)}} \prod_{i=1}^{3} \log p_i. \tag{7.25}$$

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 (7.18). Kane [38] 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

$$V_{\mathbf{a},\mathbf{k}}(n) = \frac{1}{2}\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)n^2 + O_B\left(|f_{\mathbf{a}}(\mathbf{k})|\frac{n^2}{(\log n)^B}\right), \tag{7.26}$$

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

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

in [38, Th.2]. With this choice the constant C_∞ in [38, Th.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 [38, Eq.(1.2)].

Our aim in this section is to prove the following result, conditional on the hypothesis HRH'(a_i) introduced before Theorem 7.1.3. It constitutes a version of (7.26) 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 7.2.1. *Assume* HRH'(a_i) *for* $i = 1, 2, 3$. *The following estimate holds for all square-free* k_1, k_2, k_3 *with* $1 \le k_1, k_2, k_3 \le n$ *and with an implied constant depending at most on* $\mathbf{a}$,

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

7.2.1 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 Δ_a and h_a, given in (7.4) and (7.5). We begin by determining the degree of the number field $F_{a,q,k}$ defined at the start of §7.1.3 (see [59, Lemma 2.3]).

Lemma 7.2.2. *For* k *square-free, set* $k' := k/\gcd(k, h_a)$. *Then we have*

$$[F_{a,q,k} : \mathbb{Q}] = k'\phi([q,k])/\epsilon(q,k),$$

where

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

Lemma 7.2.3. *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*

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

Proof. We have $|\mathrm{Disc}(F_{a,q,k})| = \mathfrak{N}(\Delta_{F_{a,q,k}/\mathbb{Q}(\zeta_{[q,k]})})|\mathrm{Disc}(\mathbb{Q}(\zeta_{[q,k]}))|^{[F_{a,q,k}:\mathbb{Q}(\zeta_{[q,k]})]}$, 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 it's 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 α 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,

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

Now use

$$|\mathrm{Disc}(\mathbb{Q}(\zeta_{[q,k]}))| = [q,k]^{\varphi([q,k])}\prod_{p\mid qk} p^{-\varphi([q,k])/(p-1)} \le [q,k]^{\varphi([q,k])}$$

to complete the proof. □

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 [59, Lemma 2.4]).

Lemma 7.2.4. *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 (7.10) *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 $\mathrm{Gal}(F_{a,q,k}/\mathbb{Q})$. Recall the definitions of σ_b and $c_{a,q,k}(b)$ from the start of §7.1.3.

Lemma 7.2.5. *Let $b \in \mathbb{Z}$ with $\gcd(b,q) = 1$. The following are equivalent:*

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

$$\sigma|_{\mathbb{Q}(\zeta_q)} = \sigma_b \quad \text{and} \quad \sigma|_{G_{a,k}} = \mathrm{id}_{G_{a,k}}, \tag{7.27}$$

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

3. *with $\beta_a(q)$ defined in* (7.10)*, we have*

$$b \equiv 1 \,(\mathrm{mod}\ \gcd(q,k))\,, \quad \text{and} \tag{7.28}$$

$$2 \mid k,\ \Delta_a \nmid k,\ \Delta_a \mid [q,k] \quad \text{implies that} \quad \left(\frac{\beta_a(q)}{b}\right) = 1. \tag{7.29}$$

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

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

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

Thus, an automorphism σ with (7.27) exists if and only if $c_{a,q,k}(b) = 1$, proving the equivalence of *(1)* and *(2)*. In this case σ is necessarily unique and clearly in the center of $\mathrm{Gal}(F_{a,q,k}/\mathbb{Q})$, because the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is abelian and $\mathrm{id}_{G_{a,k}}$ is in the center of $\mathrm{Gal}(G_{a,k}/\mathbb{Q})$. 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 given by $\zeta \mapsto \zeta^{b(\mathrm{mod}\ \gcd(q,k))}$, the condition (7.28) is clearly necessary. Thus, we assume it to hold from now on, whence $\sigma_b|_{\mathbb{Q}(\zeta_{\gcd(q,k)})} = \mathrm{id}_{G_{a,k}}$. If the antecedent in (7.29) is false, then we have $I = \mathbb{Q}(\zeta_{\gcd(q,k)})$ by Lemma 7.2.4, and thus $c_{a,q,k}(b) = 1$. If the antecedent in (7.29) holds, then, invoking Lemma 7.2.4 once more, we find that $\sqrt{\beta_a(q)} \in \mathbb{Q}(\zeta_q)$ and $c_{a,q,k}(b) = 1$ is equivalent to

$$\sigma_b(\sqrt{\beta_a(q)}) = \sqrt{\beta_a(q)}. \tag{7.30}$$

Since $\beta_a(q)$ is a fundamental discriminant, we may invoke [59, Lemma 2.2] to see that (7.30) is equivalent to $\left(\frac{\beta_a(q)}{b}\right) = 1$. □

7.2.2 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 $V_{\mathbf{a},\mathbf{k}}(n)$.

Lemma 7.2.6. *Assume* HRH'(a). *For any square-free k and coprime integers c, q we have*

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

Here, χ 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 χ_0. Moreover, $\tau(\chi)$ denotes the Gauss sum $\tau(\chi) = \sum_{y (\mathrm{mod}\ q)} \chi(y)\mathrm{e}_q(y)$.

Proof. We have

$$\sum_{\substack{p \le x \\ p \in \mathrm{Spl}(G_{a,k})}} (\log p)\mathrm{e}_q(cp) = \sum_{\substack{p \le x, p \nmid q \\ p \in \mathrm{Spl}(G_{a,k})}} (\log p)\mathrm{e}_q(cp) + O((\log q)^2). \tag{7.31}$$

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

$$\mathrm{e}_q(cp) = \frac{1}{\varphi(q)} \sum_{b (\mathrm{mod}\ q)} \sum_{\chi (\mathrm{mod}\ q)} \chi(b)\overline{\chi(cp)}\mathrm{e}_q(b) = \frac{1}{\varphi(q)} \sum_{\chi (\mathrm{mod}\ q)} \overline{\chi(cp)}\tau(\chi)$$

into (7.31), thus acquiring the validity of

$$\sum_{\substack{p\le x\\ p\in \mathrm{Spl}(G_{a,k})}} (\log p)\mathrm{e}_q(cp) = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi(c)}\tau(\chi)\psi_{a,k}(x,\overline{\chi}) + O((\log q)^2), \tag{7.32}$$

where

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

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 Λ 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 $e \ge 1$ 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 consider its Hecke L-function,

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

It is now easy to see that

$$-L'(s,\chi)/L(s,\chi) = \sum_{\mathfrak{n}\ne 0} \Lambda(\mathfrak{n})\chi(\mathfrak{N}\mathfrak{n})(\mathfrak{N}\mathfrak{n})^{-s}.$$

The Ramanujan–Petersson conjecture is obviously true for $L(s,\chi)$, since it is true for any Hecke L-function. Hence Theorem 5.15 from [37] implies that

$$\sum_{\mathfrak{N}\mathfrak{n}\le x} \Lambda(\mathfrak{n})\chi(\mathfrak{N}\mathfrak{n}) = r_\chi x + O(x^{\frac12}(\log x)\log(x^{[G_{a,k}:\mathbb{Q}]}\mathfrak{q}(\chi))),$$

where r_χ is the order of the pole of $L(s,\chi)$ at $s=1$. For the definition of $\mathfrak{q}(\chi)$, see page 95 of [37]. Furthermore, on page 129 of [37] it is proven that

$$\mathfrak{q}(\chi) \le 4^{[G_{a,k}:\mathbb{Q}]}|\mathrm{Disc}(G_{a,k})|q^{[G_{a,k}:\mathbb{Q}]}.$$

Our next task is to make explicit the value of r_χ. If $\chi\circ\mathfrak{N}$ is the trivial ray class character χ_0 modulo $\mathcal{O}_{G_{a,k}}$, then we have $r_\chi = 1$; otherwise we have $r_\chi = 0$. Using $|\tau(\chi)| \le \sqrt{q}$ and Lemma 7.2.3 we can substitute in (7.32) to find that

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

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

Although it is possible to directly evaluate the main term in Lemma 7.2.6, we will instead use the following trick.

Lemma 7.2.7. *Under the same conditions as in Lemma 7.2.6 we have*

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

Proof. Partitioning in progressions modulo q we see that, owing to (7.31), the sum over p in our lemma is equal to the following quantity up to an error of size $o_{q,k}(x)$,

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

By Lemma 7.2.5 there exists an automorphism σ of $F_{a,q,k}$ satisfying

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

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 7.2.6 and Lemma 7.2.7 proves the following lemma.

Lemma 7.2.8. *Under the same assumptions as in Lemma 7.2.6 we have*

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

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

$$f_{a,k}(\alpha) = \sum_{\substack{p\leq n\\ p\in \mathrm{Spl}(G_{a,k})}} (\log p)\mathrm{e}(\alpha p), \ (\alpha\in\mathbb{R}). \tag{7.33}$$

The next lemma is easily proved via partial summation and Lemma 7.2.8.

Lemma 7.2.9. *Assume* HRH'(a). *Let k be square-free integer and define $\alpha = c/q+\beta$, where $(c,q)=1$. Then*

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

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 flows directly from (7.28) and (7.29).

Lemma 7.2.10. *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 Δ_a and p_i distinct prime numbers not dividing Δ_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 7.2.11. *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 we have*

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

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 $\mathrm{e}_q(by) = \mathrm{e}_{q_1}(b_1y_1q_2)\mathrm{e}_{q_2}(b_2y_2q_1)$. This leads to

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

By Lemma 7.2.10 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

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

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

Lemma 7.2.12. *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 (7.29) always holds for $q = p^j$ as in the lemma, as the antecedent is never satisfied. We first handle the case $j = 1$. If $p \nmid k$ then by Lemma 7.2.5, $S_{a,p,k}(b)$ is the classical Ramanujan sum and the result follows, while in the remaining case, $p \mid k$, the result is also immediate from (7.28). 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

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

which is clearly sufficient since the inner sum vanishes. □

Lemma 7.2.13. *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 $f : \mathbb{Z} \to \mathbb{C}$ has period $|r|$. If we have $|r| < |Q|$ then the following sum vanishes,*

$$\sum_{b (\mathrm{mod}\ |Q|)} \mathrm{e}_{|Q|}(bc) f(b).$$

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

$$\sum_{b_0 (\mathrm{mod}\ |r|)} \mathrm{e}_{|Q|}(b_0 c) f(b_0) \sum_{x (\mathrm{mod}\ |Q/r|)} \mathrm{e}_{|Q/r|}(xc)$$

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

Lemma 7.2.14. *Let k be a square-free integer, suppose that q is composed of primes dividing Δ_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

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

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 $y \equiv 1 \bmod \gcd(k, q)$ and $\left(\frac{\beta_a(q)}{y}\right) = 1$, and $f(y) := 0$ otherwise. By Lemma 7.2.5 we have

$$S_{a,q,k}(b) = \sum_{y (\mathrm{mod}\ q)} f(y) \mathrm{e}_q(by).$$

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. Apply Lemma 7.2.13. □

Combining Lemmas 7.2.11, 7.2.12 and 7.2.14 allows us to conclude that

$$S_{a,q,k}(b) \ll 1, \tag{7.34}$$

where the implied constant depends at most on a.

7.2.3 Proof of Proposition 7.2.1

Recall (7.33). Our starting point is the circle method identity,

$$\sum_{\substack{p_1+p_2+p_3=n \\ p_i \in \mathrm{Spl}(G_{a_i,k_i})}} \prod_{i=1}^{3} (\log p_i) = \int_0^1 f_{a_1,k_1}(\alpha) f_{a_2,k_2}(\alpha) f_{a_3,k_3}(\alpha) \mathrm{e}(-n\alpha) \mathrm{d}\alpha. \tag{7.35}$$

Corollary 7.2.15. *Assume* HRH'(a), *and suppose* α, c, q *fulfil* $|\alpha - c/q| \le q^{-1}n^{-2/3}$, $\gcd(c,q) = 1$, $q \le n^{2/3}$ *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 7.2.2 gives

$$[F_{a,q,k} : \mathbb{Q}]^{-1} \ll \varphi([q,k])^{-1} \le \varphi(q)^{-1} \ll (\log q)q^{-1},$$

hence, by Lemma 7.2.9 and (7.34) 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 $q \le n^{2/3}$. □

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

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

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

Corollary 7.2.16. *Assume* HRH'(a_i) *for* $1 \le i \le 3$. *Then*

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

Proof. By Dirichlet's approximation theorem, for each α there exist coprime integers c, q with $|\alpha - c/q| \le q^{-1}n^{-2/3}$ and $1 \le q \le n^{2/3}$. If $\alpha \in \mathfrak{m}$ then $q > n^\nu$, hence Corollary 7.2.15 yields the estimate $f_{a,k}(\alpha) \ll k^2 n^{1-\nu}(\log n)^2$. We may assume $k_1 \le k_2, k_3$ with no loss of generality, therefore the integral in our lemma is

$$\ll k_1^2 n^{1-\nu}(\log n)^2 \int_0^1 |f_{a_2,k_2}(\alpha) f_{a_3,k_3}(\alpha)| \mathrm{d}\alpha,$$

thus Cauchy's inequality yields the following bound for the last integral,

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

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

Note that if $\beta + c/q \in \mathfrak{M}(q,c)$ for some $q \le n^{1/3}$ then Lemma 7.2.9 shows that

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

Hence the estimates

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

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

$$\ll \frac{\min\{n^2, |\beta|^{-2}\}}{\varphi(q)^2}\frac{n^{5/6}}{q^{1/2}}(\log n)^2 \max_i k_i^2 + \frac{n^{15/6}}{q^{3/2}}(\log n)^6 \max_i k_i^6. \tag{7.36}$$

The major arcs make the following contribution towards (7.35),

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

and a straightforward analysis utilising (7.36) reveals that the last expression equals

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

The integral over β can be estimated as $n^2/2 + O(q^2n^{4/3})$, thus by (7.34) the sum over q is $\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)n^2/2 + O((n^{4/3+\nu} + n^{2-\nu})(\log n)^3)$ and the choice $\nu = 1/6$ concludes the proof of Proposition 7.2.1.

7.3 The circle method and Hooley's approach

7.3.1 Opening phase

The aim of §7.3 is to prove Theorem 7.1.1 and Theorem 7.1.3. We commence in this subsection by calling upon parts of Hooley's work [35] 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,

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

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

$$\mathrm{N}_a(n,\eta) := \#\big\{p \le n : R_a(q,p) \text{ fails for all primes } q \le \eta\big\}$$

and

$$\mathrm{M}_a(n,\eta_1,\eta_2) := \#\big\{p \le n : \text{ there exists } q \in (\eta_1,\eta_2] \text{ such that } R_a(q,p) \text{ holds}\big\}.$$

Letting

$$\mathrm{N}_a(n) := \#\{p \le n : a \text{ is a primitive root modulo } p\}$$

we see from the work of Hooley [35, Eq.(1)] that for each $\xi_1,\xi_2,\xi_3 \in \mathbb{R}$ with

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

we have

$$\mathrm{N}_a(n) = \mathrm{N}_a(n,\xi_1) + O\big(\mathrm{M}_a(n,\xi_1,\xi_2) + \mathrm{M}_a(n,\xi_2,\xi_3) + \mathrm{M}_a(n,\xi_3,n-1)\big). \tag{7.37}$$

Hooley makes specific choices for the parameters ξ_i; we will keep the same choice for ξ_2 and ξ_3, namely $\xi_2 := n^{\frac12}(\log n)^{-2}$, $\xi_3 := n^{\frac12}\log n$, however, we shall later choose a different value for ξ_1. For the moment we shall only demand that $1 < \xi_1 \le (\log n)(\log\log n)^{-1}$. The estimates proved in [35, Eq.(2), Eq.(3)] provide us with

$$\mathrm{N}_a(n) = \mathrm{N}_a(n,\xi_1) + O\big(\mathrm{M}_a(n,\xi_1,\xi_2) + n(\log\log n)(\log n)^{-2}\big). \tag{7.38}$$

The argument in [35, Eq.(33)] shows that for each ξ_1 as above, one has under HRH(a) that

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

which, once combined with the simple estimate $\sum_{q>\xi_1} q^{-2} \ll \xi_1^{-1}$ and (7.38) provides us with

$$\mathrm{N}_a(n) = \mathrm{N}_a(n,\xi_1) + O\left(\frac{n}{\log n}\frac{1}{\xi_1} + \frac{n\log\log n}{\log^2 n}\right), \tag{7.39}$$

with an implied constant depending at most on a.

Lemma 7.3.1. *For any $\beta \in (0,1)$ and any sets of primes $\mathcal{P}_i \subset [1,n]$ of cardinality $\epsilon(\mathcal{P}_i)n/\log n$ the following estimate holds with an implied constant that depends at most on β,*

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

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

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

Straightforwardly, there exists $c = c(\beta) > 0$ with $(1-z)/(1-2z) \le (1+cz)^{1-\beta}$ for all $0 < z \le 1/3$. Using this for $z = 1/p'$ and alluding to the following classical bound (that can be found in [29, Eq. (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

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

Therefore the quantity in the lemma is

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

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 $\sum_{d \le n} \mu(d)^2 c^{\omega(d)} d^{-1} \#\{p < n : p \equiv n \pmod d\}$ we see that the contribution from integers $d > n^{1/2}$ is $\ll \sum_{n^{1/2} < d \le n} c^{\omega(d)} d^{-1}(n/d+1) \ll n^{1/2+1/100}$. By Brun–Titchmarsh, the contribution of terms with $d \le n^{1/2}$ is

$$\ll n(\log n)^{-1} \sum_{d \le n^{1/2}} c^{\omega(d)} (d\phi(d))^{-1} \ll n(\log n)^{-1},$$

thus concluding our proof. □

Let us define the set

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

The arguments bounding $\mathrm{M}_a(n, \xi_1, n-1)$ in the deduction of (7.39) show under HRH(a) that

$$\#\mathcal{P}_i \ll \frac{n}{\xi_1 \log n} + \frac{n \log\log n}{\log^2 n}. \tag{7.40}$$

We can now apply Lemma 7.3.1 and to do so let us observe that by (7.40) we have

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

Therefore, under HRH(a_i) for $i = 1, 2, 3$, and for each fixed $\beta \in (0,1)$ we acquire the validity of

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i:\ \mathbb{F}_{p_i}^* = \langle a_i \rangle}} \prod_{i=1}^3 \log p_i = \sum_{\substack{p_1+p_2+p_3=n, p_i \nmid a_i \\ \forall i, \forall q \le \xi_1:\ R_{a_i}(q,p_i) \text{ fails}}} \prod_{i=1}^3 \log p_i + O_\beta\Big(\frac{n^2}{\xi_1^\beta}\Big). \tag{7.41}$$

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

$$\mathrm{P}_{\mathbf{a},\mathbf{k}}(n) := \sum_{\substack{p_1+p_2+p_3=n,\ p_i\nmid a_i \\ \forall i:\ q\mid k_i \Rightarrow R_{a_i}(q,p_i)\ \text{holds}}} \prod_{i=1}^{3} \log p_i, \tag{7.42}$$

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

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i:\ \mathbb{F}_{p_i}^*=\langle a_i\rangle}} \prod_{i=1}^{3} \log p_i = \sum_{\substack{\mathbf{k}\in\mathbb{N}^3 \\ p\mid k_1k_2k_3 \Rightarrow p\le\xi_1}} \mu(k_1)\mu(k_2)\mu(k_3)\mathrm{P}_{\mathbf{a},\mathbf{k}}(n) + O_\beta\Big(n^2\xi_1^{-\beta}\Big). \tag{7.43}$$

The entity $\mathrm{P}_{\mathbf{a},\mathbf{k}}(n)$ is analogous to $\mathrm{P}_a(k)$ that is present in the work of Hooley [35, §3]. Indeed, the inclusion-exclusion argument above is inspired by the argument leading to [35, Eq.(5)].

Using the arguments in [35, §4] we shall first translate the $R_{a_i}(q,p_i)$-condition present in (7.42) 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 (7.5). For any positive square-free integer k_i we define $k_i' := k_i/\gcd(k_i,h_{a_i})$. Then, as explained in [35, Eq.(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 $q\mid k_i$ if and only if

$$x^{k_i'}\equiv a_i \,(\mathrm{mod}\ p)\ \text{ is soluble}\quad\text{and}\quad p\equiv 1\,(\mathrm{mod}\ k_i)\,.$$

It is then proved following [35, 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 (7.3) 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 $\gcd(h_{a_i}\gcd(k_i,h_{a_i}),k_i)\mid h_{a_i}$, hence there are integers x,y with

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

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 $\mathrm{Spl}\,(G_{a_i,k_i})$ in (7.24), we infer by (7.42) that for all $\mathbf{k}\in\mathbb{N}^3$ with each k_i square-free we have

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

for any $\beta \in (0,1)$. For the second equality, recall (7.25) and use Lemma 7.3.1. Injecting this into (7.43) we have proved that whenever $1 < \xi_1 \le (\log n)(\log\log n)^{-1}$ and $0 < \beta < 1$ then

$$\sum_{\substack{p_1+p_2+p_3=n\\ \forall i:\ \mathbb{F}_{p_i}^*=\langle a_i\rangle}} \prod_{i=1}^{3} \log p_i = \sum_{\substack{\mathbf{k}\in\mathbb{N}^3\\ p\mid k_1k_2k_3 \Rightarrow p\le\xi_1}} \mu(k_1)\mu(k_2)\mu(k_3)V_{\mathbf{a},\mathbf{k}}(n) + O_\beta\Big(n^2\xi_1^{-\beta}\Big), \tag{7.44}$$

where, for $2-\beta < \delta < 2$, the estimate

$$\begin{aligned}\sum_{\substack{\mathbf{k}\in\mathbb{N}^3\\ p\mid k_1k_2k_3\Rightarrow p\le\xi_1}} |\mu(k_1)\mu(k_2)\mu(k_3)|n^\delta &\le n^\delta\Big(\sum_{\substack{k\in\mathbb{N}\\ p\mid k\Rightarrow p\le\xi_1}} |\mu(k)|\Big)^3 = n^\delta 2^{3\#\{p\le\xi_1\}}\\ &\le n^\delta \mathrm{e}^{3\xi_1} \le n^{\delta+\frac{3}{\log\log n}}\\ &\ll_{\beta,\delta} n^2(\log n)^{-\beta}(\log\log n)^\beta \le n^2\xi_1^{-\beta}\end{aligned}$$

Before concluding the proofs of Theorem 7.1.1 and Theorem 7.1.3, we need a preparatory lemma.

Lemma 7.3.2. *The series defining $\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)$ in (7.18) and representing $\mathcal{A}_{\mathbf{a}}(n)$ in (7.19) are absolutely convergent. For each $\epsilon > 0$ and $z \ge 1$ we have*

$$\begin{aligned}\sum_{\substack{\mathbf{k}\in\mathbb{N}^3\\ \exists i,p:\ p\mid k_i \text{ and } p\ge z}} |\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)|\Big(\prod_{i=1}^{3}|\mu(k_i)|\Big) &\le \sum_{\substack{\mathbf{k}\in\mathbb{N}^3\\ \exists i:\ k_i\ge z}} \Big(\prod_{i=1}^{3}|\mu(k_i)|\Big)\sum_{q=1}^{\infty}\frac{1}{d_{\mathbf{a},\mathbf{k}}(q)}\sum_{x\in(\mathbb{Z}/q\mathbb{Z})^*}|L_{\mathbf{a},q,\mathbf{k}}(x)|\\ &\ll_\epsilon \frac{1}{z^{1-\epsilon}},\end{aligned}$$

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

Proof. The first inequality is clear by (7.18). Observe that $k_i' \ge k_i/h_{a_i} \gg k_i$, hence by Lemma 7.2.2 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 (7.34) we see by (7.18) that for $\epsilon > 0$ and square-free k_i,

$$\begin{aligned}\sum_{q=1}^{\infty}\frac{1}{d_{\mathbf{a},\mathbf{k}}(q)}\sum_{x\in(\mathbb{Z}/q\mathbb{Z})^*}|L_{\mathbf{a},q,\mathbf{k}}(x)| &\ll \prod_{i=1}^{3}\frac{1}{k_i\varphi(k_i)}\sum_{q=1}^{\infty}\frac{\varphi(\gcd(q,k_1))\varphi(\gcd(q,k_2))\varphi(\gcd(q,k_3))}{\varphi(q)^2}\\ &\ll_\epsilon \frac{\gcd(k_1,k_2,k_3)}{(k_1k_2k_3)^{2-\epsilon}}.\end{aligned}$$

Therefore, the inner sum our lemma is

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

Using the estimates

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

concludes our proof of the desired bound, which implies absolute convergence of the sum in (7.19). □

7.3.2 The proof of Theorem 7.1.1

Recall (7.26). Now note that, replacing $f_{\mathbf{a}}(\mathbf{x})$ by a larger function if necessary, we may assume in the statement of (7.26) 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, which we call $h_{\mathbf{a}}(x)$. Define the function $\xi_1 : (1,\infty)\to\mathbb{R}$ through

$$\xi_1(x) := \frac{1}{2}\cdot\min\left\{\frac{\log x}{\log\log x},\ \log(h_{\mathbf{a}}((\log x)^{B/2}))\right\} \tag{7.45}$$

and observe that

$$\lim_{x\to+\infty}\xi_1(x) = +\infty, \tag{7.46}$$

however, owing to the non-explicit error term in [38, Th.2] we cannot have any further control on the rate of divergence in the last limit. For $n\gg 1$, the definition of ξ_1 implies

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

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 injecting (7.26) into (7.44) yields the following with an implied constant depending on β and B,

$$\begin{aligned}\sum_{\substack{p_1+p_2+p_3=n\\ \forall i:\ \mathbb{F}_{p_i}^*=\langle a_i\rangle}}\prod_{i=1}^3\log p_i &= \frac{n^2}{2}\sum_{\substack{\mathbf{k}\in\mathbb{N}^3\\ p\mid k_1k_2k_3\Rightarrow p\leq\xi_1(n)}}\Big(\prod_{i=1}^3\mu(k_i)\Big)\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)+\\ &\qquad O\bigg(\frac{n^2}{\xi_1^\beta}+\frac{n^2}{(\log n)^B}\Big(\sum_{\substack{\mathbf{k}\in\mathbb{N}^3\\ \forall i:\ k_i\leq\mathrm{e}^{2\xi_1(n)}}} f_{\mathbf{a}}(\mathbf{k})\Big)\bigg)\\ &= \frac{n^2}{2}\sum_{\substack{\mathbf{k}\in\mathbb{N}^3\\ p\mid k_1k_2k_3\Rightarrow p\leq\xi_1(n)}}\Big(\prod_{i=1}^3\mu(k_i)\Big)\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)+O\bigg(\frac{n^2}{\xi_1^\beta}+\frac{n^2}{(\log n)^{B/2}}\bigg).\end{aligned}$$

An application of Lemma 7.3.2 with $\epsilon = 1 - \beta$ shows that

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

and the proof of Theorem 7.1.1 is concluded upon invoking (7.46), up to the assertion that $\mathcal{A}_{\mathbf{a}}(n) \gg_a 1$ whenever $\mathcal{A}_{\mathbf{a}}(n) > 0$. This follows immediately from Theorem 7.1.5, proved in §7.4. Moreover, we have confirmed the shape of $\mathcal{A}_{\mathbf{a}}(n)$ given in (7.19). □

Note that the reason for the non-explicit error term in Theorem 7.1.1 is that the function ξ_1 in (7.45) is not explicit.

7.3.3 The proof of Theorem 7.1.3

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

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

Injecting Proposition 7.2.1 into (7.44) provides us with

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i:\ \mathbb{F}_{p_i}^*=\langle a_i\rangle}} \prod_{i=1}^{3} \log p_i - \frac{n^2}{2} \sum_{p|k_1k_2k_3\Rightarrow p\le\xi_1} \mathfrak{S}_{\mathbf{a},\mathbf{k}}(n) \prod_{i=1}^{3} \mu(k_i) \ll_\beta \frac{n^2}{\xi_1^\beta} + \frac{(\log n)^6}{n^{-11/6}} \Big(\sum_{\substack{k\in\mathbb{N} \\ p|k\Rightarrow p\le\xi_1}} k^6|\mu(k)|\Big)^3.$$

For $n \gg 1$, each k in the sum satisfies $k \le \prod_{p\le\xi_1} p \le n^{\frac{2}{\log\log n}}$, hence the cube of the sum over k is at most $n^{\frac{\theta}{\log\log n}}$ for some absolute positive constant θ. This shows that the right side above is $\ll_\beta n^2\xi_1^{-\beta}$. Appealing to Lemma 7.3.2 completes the proof of Theorem 7.1.3. □

7.4 Artin's factor for ternary Goldbach

In this section, we study in detail the leading factor $\mathcal{A}_{\mathbf{a}}(n)$ in Theorems 7.1.1 and 7.1.3, and thus prove Theorem 7.1.5, Corollary 7.1.6 and Theorem 7.1.7. Recall that we have already confirmed the equality (7.19) in the proof of Theorem 7.1.1 in §7.3.2.

7.4.1 The proof of (7.22)

Recall the definitions of $F_{a,q,k}(b)$ and $c_{a,q,k}(b)$ from the start of §7.1.3. It was shown by Lenstra [51, Th.(3.1),Eq.(2.15)] conditionally under HRH(a), that for all integers b and $q > 0$ the Dirichlet density of the primes p satisfying the following conditions exists,

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

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 [59], who showed that

$$\sum_{k\in\mathbb{N}} \frac{\mu(k)c_{a,q,k}(b)}{[F_{a,q,k} : \mathbb{Q}]} = \delta_a(b \bmod q), \tag{7.47}$$

where $\delta_a(b \bmod q)$ is the arithmetic function given in Definition 7.1.4. We will make consistent use of Moree's result in this section.

Lemma 7.4.1. *We have*

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

Proof. Recall (7.15) and (7.18). Lemma 7.3.2 allows us to rearrange terms, thus we can rewrite the sum over $\mathbf{k}$ in our lemma as

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

By (7.15) the sum over k_i equals

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

and using (7.47) concludes our proof. □

The difficulty of converting the sum over $\mathbf{k}$ in (7.19) into a product comes from the fact that the terms $\delta_{a_i}(b_i \bmod q)$ in Lemma 7.4.1 are not a multiplicative function of q. These terms would be multiplicative in the classical Vinogradov setting, where one has $\mathbf{1}_{\gcd(b_i,q)=1}(b_i)/\phi(q)$ in place of $\delta_{a_i}(b_i \bmod q)$.

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

Lemma 7.4.2. *If the odd part of a positive integer q is not square-free then the following expression vanishes,*

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

Furthermore, the expression vanishes if $\nu_2(q) > \min\{\nu_2(\Delta_i) : i = 1, 2, 3\}$.

Proof. In the present proof we write $[P] := 1$ if a proposition P holds, and $[P] := 0$ otherwise. For $1 \le i \le 3$, we factorise each positive integer q as $q = q_{i,0}q_{i,1}$, where the positive integers $q_{i,0}, q_{i,1}$ are uniquely defined through the conditions $p \mid q_{i,0} \Rightarrow p|\Delta_i$ and $\gcd(q_{i,1}, \Delta_i) = 1$. Now owing to Definition 7.1.4 the quantity $\delta_{a_i}(b_i \bmod q)/\mathcal{A}_{a_i}$ equals

$$\Bigg(\big[\gcd(b_i, q_{i,1})\gcd(b_i - 1, q_{i,1}, h_{a_i}) = 1\big] \frac{f_{a_i}^{\dagger}(q_{i,1})}{\phi(q_{i,1})} \prod_{p|b_i-1, p|q_{i,1}} \Big(1 - \frac{1}{p}\Big) \Bigg) \times$$
$$\Bigg(\frac{f_i^{\dagger}(q_{i,0})}{\phi(q_{i,0})} \prod_{p|b_i-1, p|q_{i,0}} \Big(1 - \frac{1}{p}\Big) \Bigg) \times \big[\gcd(b_i, q_{i,0})\gcd(b_i - 1, q_{i,0}, h_{a_i}) = 1\big] \times$$
$$\Bigg(1 + \Big(\frac{\beta_i(q_{i,0})}{b_i}\Big) \mu\Big(\frac{2|\Delta_i|}{\gcd(q_{i,0}, \Delta_i)}\Big) f_{a_i}^{\ddagger}\Big(\frac{|\Delta_i|}{\gcd(q_{i,0}, \Delta_i)}\Big) \Bigg).$$

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

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

and

$$\sum_{\substack{b_{i,0} (\bmod\ q_{i,0}) \\ \gcd(b_{i,0}, q_{i,0}) = 1 \\ \gcd(b_{i,0}q_{i,1} - 1, q_{i,0}, h_{a_i}) = 1}} \frac{\mathrm{e}(b_{i,0}c/q_{i,0})}{\prod_{p|(b_{i,0}q_{i,1}-1, q_{i,0})}(1 - \frac{1}{p})^{-1}} \times$$
$$\Bigg(1 + \Big(\frac{\beta_i(q_{i,0})}{b_{i,0}q_{i,1}}\Big) \mu\Big(\frac{2|\Delta_i|}{\gcd(q_{i,0}, \Delta_i)}\Big) f_{a_i}^{\ddagger}\Big(\frac{|\Delta_i|}{\gcd(q_{i,0}, \Delta_i)}\Big) \Bigg).$$

To study the sum over $b_{i,1}$ we use Lemma 7.2.13 with

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

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 $\nu_p(q) = \nu_p(q_{i,1}) \le 1$.

Now the sum over $b_{i,0}$ can be studied via Lemma 7.2.13 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

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

We have used the fact that $p \mid q_{i,0} \Leftrightarrow p \mid r$ and that the Kronecker symbol has period $|\beta(q_{i,0})| = r$. Lemma 7.2.13 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 $q_{i,0} \mid \Delta_i$. Now if a prime p satisfies $p \mid \gcd(\Delta_1, \Delta_2, \Delta_3)$ we have that for every i, $\nu_p(q) = \nu_p(q_{i,0}) \leq \nu_p(\Delta_i)$, thus $\nu_p(q) \leq \min\{\nu_p(\Delta_i) : i = 1, 2, 3\}$. If $p \neq 2$ then this shows that $\nu_p(q) \leq 1$ since the odd part of a fundamental discriminant is square-free, while if $p = 2$ then we must have $\nu_2(q) \leq \min\{\nu_2(\Delta_i) : i = 1, 2, 3\}$. □

Lemma 7.4.2 allows us to simplify the summation over q in Lemma 7.4.1 since the only integers q making a contribution towards the sum must satisfy

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

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

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

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

$$\gcd(q(\mathbf{w}), \prod_{i:\mathbf{w}(i)=1} \Delta_i) = 1 \quad \text{and} \quad q(\mathbf{w}) \mid \gcd\{\Delta_i : \mathbf{w}(i) = 0\}. \tag{7.48}$$

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 have $\mathbf{w} \notin \{(0,0,0),(1,1,1)\} \Rightarrow q(\mathbf{w}) = 1$. We now use the definition of $q(\mathbf{w})$, Lemma 7.4.1 and Lemma 7.4.2 to infer

$$\sum_{\mathbf{k} \in \mathbb{N}^3} \mu(k_1)\mu(k_2)\mu(k_3)\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n) = \sum_{\substack{(q(\mathbf{w})) \in \mathbb{N}^8, \\ (7.48) \text{ holds} \\ \mu(q((1,1,1)))^2=1}} \sum_{\substack{c \pmod{\prod_{\mathbf{w}} q(\mathbf{w})} \\ \gcd(c, \prod_{\mathbf{w}} q(\mathbf{w}))=1}} \mathrm{e}(-nc \prod_{\mathbf{w}} q(\mathbf{w})^{-1}) \times$$
$$\prod_{i=1}^{3} \left(\sum_{b_i \pmod{\prod_{\mathbf{w}} q(\mathbf{w})}} \mathrm{e}\Big(b_i c \prod_{\mathbf{w}} q(\mathbf{w})^{-1}\Big) \delta_{a_i}\Big(b_i \bmod \prod_{\mathbf{w}} q(\mathbf{w})\Big) \right). \tag{7.49}$$

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

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

and recalling Definition 7.1.4 we see that

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

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

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

For the further analysis of the expressions above, we introduce for $r \in \mathbb{N}$, $c \in \mathbb{Z}$ the quantity

$$\mathcal{M}_a(c,r) := \frac{1}{\mathcal{A}_a} \sum_{b \pmod r} \mathrm{e}_r(bc)\mathcal{A}_a(b \bmod r), \tag{7.50}$$

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

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

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

$$\mathcal{A}_{a_i}^{-1} \sum_{b_i'' \pmod{\prod_{\mathbf{w}(i)=1} q(\mathbf{w})}} \mathrm{e}\Big(b_i'' c \prod_{\mathbf{w}(i)=1} q(\mathbf{w})^{-1}\Big)\mathcal{A}_{a_i}\Big(b_i'' \prod_{\mathbf{w}(i)=0} q(\mathbf{w}) \bmod \prod_{\mathbf{w}(i)=1} q(\mathbf{w})\Big)$$

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

$$\sum_{b_i' \pmod{\prod_{\mathbf{w}(i)=0} q(\mathbf{w})}} \mathrm{e}\Big(b_i' c \prod_{\mathbf{w}(i)=0} q(\mathbf{w})^{-1}\Big)\delta_{a_i}\Big(b_i' \prod_{\mathbf{w}(i)=1} q(\mathbf{w}) \bmod \prod_{\mathbf{w}(i)=0} q(\mathbf{w})\Big).$$

Let us bring into play the entities

$$\Delta_{\mathbf{w}} := \prod_{p \nmid \prod_{\mathbf{w}(i)=1} \Delta_i} p^{\min\{\nu_p(\Delta_i)\,:\,\mathbf{w}(i)=0\}},$$

which we interpret as 1 in case $\mathbf{w} = (1,1,1)$, and note that $\prod_{\mathbf{w}} \Delta_{\mathbf{w}}$ coincides with the

entity $\mathfrak{D}_{\mathbf{a}}$ introduced in (7.21). We see that the sum in (7.49) becomes

$$\sum_{\substack{(q(\mathbf{w}))\in\mathbb{N}^8\\ \mathbf{w}\neq(1,1,1)\Rightarrow q(\mathbf{w})|\Delta_{\mathbf{w}}\\ \mu(q((1,1,1)))^2=1\\ \gcd(q((1,1,1)),\Delta_1\Delta_2\Delta_3)=1}} \sum_{(c^{[\mathbf{w}]})\in\prod_{\mathbf{w}}(\mathbb{Z}/q(\mathbf{w})\mathbb{Z})^*} \Big(\prod_{\mathbf{w}} \mathrm{e}_{q(\mathbf{w})}(-nc^{[\mathbf{w}]})\Big)\times$$

$$\times\prod_{i=1}^{3}\Big\{\mathcal{D}_{a_i}((c^{[\mathbf{w}]})_{\mathbf{w}(i)=0},(q(\mathbf{w}))_{\mathbf{w}(i)=0})\prod_{\mathbf{w}(i)=1}\mathcal{M}_{a_i}(c^{[\mathbf{w}]},q(\mathbf{w}))\Big\}.$$

Clearly, the terms corresponding to $q((1,1,1))$ can be separated, thus, in light of (7.49), we are led to

$$\sum_{\mathbf{k}\in\mathbb{N}^3}\mu(k_1)\mu(k_2)\mu(k_3)\mathfrak{S}_{\mathbf{a},\mathbf{k}}(n)=S_{\mathbf{a},0}(n)S_{\mathbf{a},1}(n), \tag{7.51}$$

where

$$S_{\mathbf{a},0}(n):=\sum_{\substack{(q(\mathbf{w}))_{\mathbf{w}\neq(1,1,1)}\in\mathbb{N}^7\\ q(\mathbf{w})|\Delta_{\mathbf{w}}}}\sum_{(c^{[\mathbf{w}]})\in\prod_{\mathbf{w}\neq(1,1,1)}(\mathbb{Z}/q(\mathbf{w})\mathbb{Z})^*}\Big(\prod_{\mathbf{w}\neq(1,1,1)}\mathrm{e}_{q(\mathbf{w})}(-nc^{[\mathbf{w}]})\Big)\times$$

$$\prod_{i=1}^{3}\Big\{\mathcal{D}_{a_i}((c^{[\mathbf{w}]})_{\mathbf{w}(i)=0},(q(\mathbf{w}))_{\mathbf{w}(i)=0})\prod_{\substack{\mathbf{w}(i)=1\\ \mathbf{w}\neq(1,1,1)}}\mathcal{M}_{a_i}(c^{[\mathbf{w}]},q(\mathbf{w}))\Big\}$$

and

$$S_{\mathbf{a},1}(n):=\sum_{\gcd(q((1,1,1)),\Delta_1\Delta_2\Delta_3)=1}\mu(q((1,1,1)))^2\times$$

$$\sum_{c^{[(1,1,1)]}\in(\mathbb{Z}/q((1,1,1))\mathbb{Z})^*}\mathrm{e}_{q((1,1,1))}(-nc^{[(1,1,1)]})\prod_{i=1}^{3}\mathcal{M}_{a_i}(c^{[(1,1,1)]},q((1,1,1))). \tag{7.52}$$

Lemma 7.4.3. *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

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

If we assume HRH(a_i) then it is immediately clear from Moree's interpretation of δ_{a_i} as Dirichlet densities [59] that the following holds,

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

One can also prove this unconditionally directly from Definition 7.1.4 via a tedious but straightforward calculation that we do not reproduce here. To conclude the proof we observe that

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

(2): Due to the assumption that $\mathbf{w}(i) = 1$ 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 conducted 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 (7.20) and use the following lemma.

Lemma 7.4.4. *If $p \nmid \Delta_1\Delta_2\Delta_3$, then*

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

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

$$\sum_{c\in\mathbb{Z}/p\mathbb{Z}} \mathrm{e}_p(-cn)\prod_{i=1}^{3}\mathcal{M}_{a_i}(c,p) = \sum_{\mathbf{b}\in(\mathbb{Z}/p\mathbb{Z})^3}\Big(\prod_{i=1}^{3}\frac{\mathcal{A}_{a_i}(b_i \mathrm{mod}\ p)}{\mathcal{A}_{a_i}}\Big) \sum_{c\in\mathbb{Z}/p\mathbb{Z}} \mathrm{e}_p(c(b_1+b_2+b_3-n)),$$

which is in turn equal to

$$p \sum_{\substack{\mathbf{b}\in(\mathbb{Z}/p\mathbb{Z})^3\\ \sum_{i=1}^{3} b_i\equiv n(\mathrm{mod}\ p)}} \prod_{i=1}^{3}\frac{\mathcal{A}_{a_i}(b_i \mathrm{mod}\ p)}{\mathcal{A}_{a_i}}.$$

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

Using (7.52), multiplicativity and Lemma 7.4.4, we infer that

$$S_{\mathbf{a},1}(n) = \prod_{p\nmid\Delta_1\Delta_2\Delta_3}\Big(1+\sum_{c\in(\mathbb{Z}/p\mathbb{Z})^*}\mathrm{e}_p(-nc)\prod_{i=1}^{3}\mathcal{M}_{a_i}(c,p)\Big) = \prod_{p\nmid\Delta_1\Delta_2\Delta_3}\sigma_{\mathbf{a},n}(p). \tag{7.53}$$

We now turn our attention to $S_{\mathbf{a},0}(n)$. Letting $d_{\mathbf{w}} := \Delta_{\mathbf{w}}/q(\mathbf{w})$ we use Lemma 7.4.3 to obtain

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

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

$$y^{[\mathbf{w}]} = c^{[\mathbf{w}]}d_{\mathbf{w}}, \quad c^{[\mathbf{w}]} \in \Big(\frac{\mathbb{Z}}{(\Delta_{\mathbf{w}}/d_{\mathbf{w}})\mathbb{Z}}\Big)^*.$$

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

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

By definition, $\Delta_{(1,1,1)} = 1$, so $\mathfrak{D}_{\mathbf{a}} = \prod_{\mathbf{w}\neq(1,1,1)} \Delta_{\mathbf{w}}$. Note that $\gcd(\Delta_{\mathbf{w}}, \Delta_{\mathbf{v}}) = 1$ for $\mathbf{w} \neq \mathbf{v}$. Using the Chinese remainder theorem and writing every $y \left(\mathrm{mod}\ \prod_{\mathbf{v}\neq(1,1,1)} \Delta_{\mathbf{w}}\right)$ as

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

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

$$\sum_{y(\mathrm{mod}\ \mathfrak{D}_{\mathbf{a}})} \mathrm{e}(-ny/\mathfrak{D}_{\mathbf{a}}) \prod_{i=1}^{3} \left(\sum_{b_i(\mathrm{mod}\ \mathfrak{D}_{\mathbf{a}})} \mathrm{e}(b_i y/\mathfrak{D}_{\mathbf{a}}) \delta_{a_i}(b_i \bmod \mathfrak{D}_{\mathbf{a}}) \right).$$

This is clearly

$$\mathfrak{D}_{\mathbf{a}} \sum_{\substack{\mathbf{b}(\mathrm{mod}\ \mathfrak{D}_{\mathbf{a}}) \\ \sum_{i=1}^{3} b_i \equiv n (\mathrm{mod}\ \mathfrak{D}_{\mathbf{a}})}} \prod_{i=1}^{3} \delta_{a_i}(b_i \bmod \mathfrak{D}_{\mathbf{a}}),$$

thus, recalling (7.20), we have shown that

$$S_{\mathbf{a},0}(n) = \sigma_{\mathbf{a},n}(\mathfrak{D}_{\mathbf{a}}) \prod_{i=1}^{3} \mathcal{L}_{a_i}. \tag{7.54}$$

The proof of (7.22) is concluded upon combining (7.51), (7.53) and (7.54).

7.4.2 The proof of (7.23)

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 7.4.5. *For an integer c and a prime p with $p \nmid c$ we have*

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

Proof. Combining (7.12) and (7.50) we immediately infer

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

It is now easy to see that the sum over b equals $-1-\mathrm{e}_p(c)$ or $-1-\mathrm{e}_p(c)/p$ 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 7.4.6. *For every odd integer n and prime $p \nmid \prod_{i=1}^{3} \Delta_i$ we have*

$$\sigma_{\mathbf{a},n}(p) = 1 - \frac{p}{\prod_{1\le i\le 3}(p-1-\theta_{a_i}(p))}\Big(\sum_{\substack{0\le j\le 3\\ j\equiv n(\mathrm{mod}\ p)}} \Xi_j(p)\Big) + \prod_{1\le i\le 3}\Big(\frac{1+\theta_{a_i}(p)}{p-1-\theta_{a_i}(p)}\Big).$$

Proof. By Lemma 7.4.4 and Lemma 7.4.5 we see that

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

The sum over c equals

$$\sum_{0\le j\le 3}\Xi_j(p)\sum_{c\in(\mathbb{Z}/p\mathbb{Z})^*}\mathrm{e}_p(c(j-n)) = p\Big(\sum_{\substack{0\le j\le 3\\ j\equiv n(\mathrm{mod}\ p)}}\Xi_j(p)\Big) - \prod_{1\le i\le 3}(1+\theta_{a_i}(p))$$

and the proof is complete. □

Lemma 7.4.7. *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* $n \equiv 1 \,(\mathrm{mod}\ 3)$.

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 $p \ge 5$ there exists at most one $0 \le j \le 3$ satisfying $j \equiv n \,(\mathrm{mod}\ p)$, therefore

$$\sum_{\substack{0\le j\le 3\\ j\equiv n(\mathrm{mod}\ p)}}\Xi_j(p) \le 3.$$

Invoking Lemma 7.4.6 we obtain

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

Recall that no a_i is a square, hence $2 \nmid h_{a_1} h_{a_2} h_{a_3}$. The fact that n is odd implies that

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

hence if $\Delta_1\Delta_2\Delta_3$ is odd we can use Lemma 7.4.6 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, in the case that $n \equiv 1 \pmod 3$ we have

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

and we can check that $\sigma_{\mathbf{a},n}(3) = 0$ if and only if at most one of the θ_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 $(\theta_{a_i}(3))_i \in \{1, \frac{1}{3}\}^3$, 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 (7.54). 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 7.4.6. We shall instead opt to bound the densities $\delta_a(b_i \bmod \mathfrak{D}_{\mathbf{a}})$ from below in (7.54) and then count the number of solutions of the equation $n \equiv x_1 + x_2 + x_3 \pmod{\mathfrak{D}_{\mathbf{a}}}$ such that for every i we have $\delta_a(x_i \bmod \mathfrak{D}_{\mathbf{a}}) \neq 0$.

Lemma 7.4.8. *For any integers q and x such that q is positive and $\delta_a(x \bmod q) > 0$ we have*

$$\delta_a(x \bmod q) \gg \frac{\phi(h_a)}{q h_a},$$

with an absolute implied constant.

Proof. Under the assumptions of our lemma we have the following due to Definition 7.1.4,

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

The right-hand side is either ≥ 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

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

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

Recalling (7.20) we see that

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

thus, if $\sigma_{\mathbf{a},n}(\mathfrak{D}_{\mathbf{a}}) > 0$ then there exist $x_1, x_2, x_3 \,(\mathrm{mod}\ \mathfrak{D}_{\mathbf{a}})$ such that

$$\prod_{i=1}^{3}\delta_{a_i}(x_i \bmod \mathfrak{D}_{\mathbf{a}}) > 0$$

and $x_1+x_2+x_3 \equiv n \,(\mathrm{mod}\ \mathfrak{D}_{\mathbf{a}})$. Invoking Lemma 7.4.8 we see that if $\sigma_{\mathbf{a},n}(\mathfrak{D}_{\mathbf{a}}) > 0$ then

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

Recalling (7.21) we obtain $\mathfrak{D}_{\mathbf{a}} \leq [\Delta_1,\Delta_2,\Delta_3] \leq |\Delta_1\Delta_2\Delta_3|$, hence

$$\sigma_{\mathbf{a},n}(\mathfrak{D}_{\mathbf{a}})\prod_{i=1}^{3}\mathcal{L}_{a_i} \gg \prod_{i=1}^{3}\frac{\phi(h_{a_i})}{|\Delta_i|^2 h_{a_i}}, \tag{7.55}$$

with an absolute implied constant. Combined with Lemma 7.4.7, this concludes the proof of (7.23).

7.4.3 The proof of Theorem 7.1.5

The proof of the first part of Theorem 7.1.5, which is (7.22) is spread throughout §7.4.1. The proof of the second (and last) part of Theorem 7.1.5, which is (7.23), is spread throughout §7.4.2.

7.4.4 The proof of Corollary 7.1.6

Obviously, *(1)* implies *(2)*. For the reverse direction, let $d \in \{3, \mathfrak{D}_{\mathbf{a}}\}$ 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

$$p_1 + p_2 + p_3 \equiv n \bmod d.$$

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 [51, p.g.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 (7.20) shows that $\sigma_{\mathbf{a},n}(\mathfrak{D}_{\mathbf{a}})\sigma_{\mathbf{a},n}(3) > 0$. By Lemma 7.4.7, we get $\mathcal{A}_{\mathbf{a}}(n) > 0$, and thus $\mathcal{A}_{\mathbf{a}}(n) \gg 1$ by (7.23). Thus, *(1)* follows immediately from Theorem 7.1.1 and the trivial estimate

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

7.4.5 The proof of Theorem 7.1.7

First note that $\mathfrak{D}_{(a,a,a)} = |\Delta_a|$. It is clear that for the proof of Theorem 7.1.7 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 7.4.7 the condition $\prod_{p \nmid \Delta_a} \sigma_{(a,a,a),n}(p) \neq 0$ is equivalent to

$$\begin{cases} n \equiv 3 \pmod 6, & \text{if } 3 \mid h_a \text{ and } 3 \nmid \Delta_a, \\ n \equiv 1 \pmod 2, & \text{otherwise.} \end{cases} \tag{7.56}$$

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

Proposition 7.4.9. *Assume that n is an odd positive integer.*

1. *If $3 \nmid \gcd(\Delta_a, h_a)$ or $3 \mid n$, and if Δ_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 7.1.4 that the quantity $\delta_a(x_i \bmod |\Delta_a|)$ is non-zero if and only if

$$\gcd(x_i - 1, \Delta_a, h_a) = 1,\ \gcd(x_i, \Delta_a) = 1 \text{ and } \left(\frac{\Delta_a}{x_i}\right) = -1. \tag{7.57}$$

In view of Definition 7.20, we need to find conditions under which there are $x_1, x_2, x_3 \in \mathbb{Z}$ with $x_1 + x_2 + x_3 \equiv n \bmod \Delta_a$, such that each x_i satisfies (7.57).

To prove *(2)*, we observe that the first two conditions in (7.57) imply that $x_i \equiv 2 \bmod 3$, hence $3 \mid n$.

Let us now prove *(1)*. We can write $\Delta_a = \prod_{p|\Delta_a} D_p$, 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 Δ_a. For every $p < p'$, we find $x_1^{(p)}, x_2^{(p)}, x_3^{(p)} \bmod D_p$ that solve the congruence $x_1^{(p)}+x_2^{(p)}+x_3^{(p)} \equiv n \bmod D_p$ 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

$$R := \Big\{x \in \mathbb{Z}/p'\mathbb{Z} : \left(\frac{x}{p'}\right) = 1, x \neq 1 \,(\mathrm{mod}\ p')\Big\},\ N := \Big\{x \in \mathbb{Z}/p'\mathbb{Z} : \left(\frac{x}{p'}\right) = -1\Big\}.$$

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

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

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 $x_i \equiv x_i^{(p)} \bmod D_p$ 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 (7.57), and moreover $x_1 + x_2 + x_3 \equiv n \bmod \Delta_a$. □

Proof of Theorem 7.1.7. 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 Δ_a and it is straightforward to use a computer program that finds all congruence classes $n \,(\mathrm{mod}\ \Delta_a)$ such that $n \equiv x_1 + x_2 + x_3 \,(\mathrm{mod}\ \Delta_a)$ for some $\mathbf{x} \in (\mathbb{Z}/\Delta_a\mathbb{Z})^3$ satisfying all of the conditions (7.57) for $1 \leq i \leq 3$.

By Definition 7.1.4 these conditions are equivalent to $\delta_a(x_i \bmod |\Delta_a|) \neq 0$ and when combined with (7.56) they provide the congruence classes for n in every row of the table in Theorem 7.1.7 apart from the last two rows. For the last two rows, Δ_a has a prime factor greater than 7, so one sees by Proposition 7.4.9 that we only have to provide conditions on n that are equivalent to $\prod_{p\nmid\Delta_a} \sigma_{(a,a,a),n}(p) > 0$, which was already done in (7.56). □

7.4.6 Non-factorisation of $\mathcal{A}_{\mathbf{a}}(n)$

We finish by showing that the right side in (7.22) 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 $\lambda_a : \mathbb{Z}^2 \to [0, \infty)$ such that for every prime p and integers x, x' we have

$$\delta_a(x \bmod p) > 0 \Rightarrow \lambda_a(x, p) > 0 \tag{7.58}$$

and

$$x \equiv x' \,(\mathrm{mod}\ p) \Rightarrow \lambda_a(x, p) = \lambda_a(x', p).$$

Now, in parallel with (7.20) let us define

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

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

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

$$\mathcal{L}_a^3 \sigma_{(a,a,a),n}(|\Delta_a|) = \prod_{p|\Delta_a} \varpi_{p,a}(n). \tag{7.59}$$

Indeed, if $a := (-15)^5 = -759375$ then by Definition 7.1.4 we easily see that

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

hence for all integers $n \equiv 7 \,(\mathrm{mod}\ 15)$ we have $\sigma_{(a,a,a),n}(|\Delta_a|) = 0$ due to (7.20) and the fact that for all $\mathbf{x} \in \{7, 13, 14\}^3$ one has $\sum_{i=1}^3 x_i \neq 7 \,(\mathrm{mod}\ 15)$. Definition 7.1.4 furthermore implies that

$$\delta_{-759375}(x \bmod 3) > 0 \Leftrightarrow x \,(\mathrm{mod}\ 3) \in \{1, 2 \,(\mathrm{mod}\ 3)\}$$

and

$$\delta_{-759375}(y \bmod 5) > 0 \Leftrightarrow y \,(\mathrm{mod}\ 5) \in \{2, 3, 4 \,(\mathrm{mod}\ 5)\},$$

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

$$\sum_{i=1}^{3} x_i \equiv n \,(\mathrm{mod}\ 3), \quad \sum_{i=1}^{3} y_i \equiv n \,(\mathrm{mod}\ 5)$$

and

$$\prod_{i=1}^{3} \delta_{-759375}(x_i \bmod 3) \delta_{-759375}(y_i \bmod 5) > 0.$$

By (7.58) this implies that $\varpi_{3,-759375}(n) > 0$ and $\varpi_{5,-759375}(n) > 0$. This contradicts equation (7.59) due to $\sigma_{(a,a,a),n}(|\Delta_a|) = 0$.