The Largest Prime Factor of $X^3 + 2$

D.R. Heath-Brown
Mathematical Institute, Oxford

1 Introduction

It is conjectured that if $f(X)$ is an irreducible integer polynomial with positive leading coefficient, then $f(n)$ takes infinitely many prime values, providing only that $f(n)$ has no fixed prime divisor. As an approximation to this conjecture one might ask whether $f(n)$ has a very large prime factor in infinitely many cases. To make this more precise, we shall define $P(x; f)$ to be the largest prime factor of

$$\prod_{n \le x} f(n)$$

and ask for lower bounds for $P(x; f)$.

The first non-trivial result in this direction was found by Chebyshev, and states that

$$\frac{P(x; X^2 + 1)}{x} \to \infty.$$

The proof was sketched in Chebyshev's posthumous manuscripts. The result was published and proved in full by Markov [8]. It was later sharpened and generalized by Nagell [9] who showed that

$$P(x; f) \gg x(\log x)^\theta$$

for any fixed irreducible polynomial $f(X)$, and any constant $\theta < 1$. Further strengthenings of this latter result were obtained by Erdős [2] who showed that

$$P(x; f) \gg x(\log x)^{A \log\log\log x}$$

for a suitable constant $A > 0$, and Tenenbaum [10], who obtained

$$P(x; f) \gg x \exp\{(\log x)^A\}$$

for any constant $A < 2 - \log 4 = 0.61\ldots$. This is the best result currently available for polynomials of arbitrary degree. However for the specific case $f(X) = X^2 + 1$ Hooley [5] was able to show that

$$P(x; X^2 + 1) \gg x^{11/10}.$$

Indeed Hooley's method handles $X^2 - D$ for any non-square integer D, and presumably can be generalized to arbitrary irreducible quadratic polynomials. In the case of the polynomial $X^2 + 1$ the exponent $11/10$ was improved by Deshouillers and Iwaniec [1], to the root $\theta = 1.202\ldots$ of the equation $\theta + 2\log(2 - \theta) = 3/4$. Again one can handle $X^2 - D$ for any non-square D.

Until now, no corresponding result for cubic polynomials has been established. However Hooley [6] succeeded in giving a conditional proof that

$$P(x; X^3 + 2) \gg x^{1+\delta}$$

for some constant $\delta > 0$, assuming certain estimates for short Ramanujan-Kloosterman sums. Indeed under the best possible hypothesis of this type, the 'R^* Hypothesis', Hooley showed that $\delta = 1/30$ would be admissible. The purpose of the present paper is to give an unconditional treatment of such an estimate.

Theorem 1 *Let $\varpi = 10^{-303}$ and suppose that X is sufficiently large. Then, for at least a positive proportion of the integers $n \in (X, 2X]$, the number $n^3 + 2$ has a prime factor in excess of $X^{1+\varpi}$. In particular we have*

$$P(x; X^3 + 2) \gg x^{1+\varpi}.$$

The constant ϖ is indeed barely positive. It seems likely that the exponent 303 could be reduced very considerably. The proof we shall present is designed to be as simple as possible while still producing an explicit value for ϖ. There is much scope for optimising the argument. In particular there is one point in our analysis at which ϖ^{-1} depends exponentially on a certain parameter. With more care a polynomial bound may be given.

It would be interesting to know whether the result could be generalized to other irreducible cubic polynomials. It seems likely that this can be done, the only serious difficulties arising in §3. Indeed one may also ask whether higher degree polynomials might be successfully treated. As yet it is still not clear that such an extension is impossible.

In [6] Hooley was able to show how solutions of the congruence $X^2 + 2 \equiv 0 \pmod{n}$ could be related to the representations of n by the norm form $X^3 + 2Y^3 + 4Z^3 - 6XYZ$, just as Gauss had done for the theory of binary quadratic forms. We have preferred an alternative formulation in terms of the theory of ideals in $\mathbb{Q}(\sqrt[3]{2})$. We do this principally because we believe that it will be more familiar to readers, the two approaches being largely equivalent. Whichever line of attack one chooses, the transition from solutions of a polynomial congruence modulo n to a representation of n by a norm form will be a cornerstone of the agrument.

Hooley's approach, which began with Chebyshev's basic idea, gave rise to sums of the form

$$\sum_{A < n \leq A+B} e_q(\overline{n}^{(q)}),$$

where $e_q(m) = \exp(2\pi i m/q)$ and $n\overline{n}^{(q)} \equiv 1 \pmod{q}$. (Only values of n for which $(q, n) = 1$ are to be included above.) For these sums it was necessary to have a non-trivial bound when B was roughly of size $q^{1/3}$. No such bound is currently available, and Hooley was therefore forced to rely on an unproved hypothesis at this point.

Our work will use an estimate of the type assumed by Hooley, which holds providing that q factorizes suitably. It must however be emphasized that the values of q arising in Hooley's work do not automatically have suitable factorizations. It is therefore necessary to revise the basic approach to our problem very considerably. Indeed our new method is applicable, in principle, to a large

number of questions for which Chebyshev's method has been used. This will be discussed in the final section of the paper.

To estimate short Ramanujan-Kloosterman sums, we shall use what we have termed the 'q-analogue of van der Corput's method', the principles of which were described by the author [4]. Since it requires little extra effort, we shall establish a result more general than is needed for the current application. This will concern sums

$$S = \sum_{A<n\le A+B} e_q(f(n)\overline{g(n)}^{(q)}),$$

with integral A and B, involving a general rational function $f(n)/g(n)$, interpreted modulo q. In writing such sums we shall adopt the convention that only values of n for which $(g(n), q) = 1$ are to be included in the summation.

Theorem 2 *Let $q = q_0q_1 \dots q_k$ be a positive square-free integer. Suppose that $f(X), g(X)$ are integral polynomials with $\deg(f(X)), \deg(g(X)) \le D$. Assume that for every prime factor p of q we have $p > 2^kD$. Moreover for all $p|q$, suppose that there is no polynomial $h(X)$, with $\deg(h(X)) \le k+1$, for which $f(X) \equiv g(X)h(X) \pmod p$. (In particular we must have $p \nmid f(X)$.) Then, for any $\varepsilon > 0$ we have*

$$\sum_{A<n\le A+B} e_q(wf(n)\overline{g(n)}^{(q)})$$

$$\ll_{k,D,\varepsilon} \quad q^{\varepsilon}\{B(\frac{\Delta}{q_0})^{1/2^{k+1}} + B^{1-1/2^k}(\frac{q_0}{\Delta})^{1/2^{k+1}} + \sum_{j=1}^{k} B^{1-1/2^j} q_{k+1-j}^{1/2^j}\},$$

where $\Delta = (q_0, w)$.

It may be instructive to examine the case in which $\Delta = 1$ and the factors q_i satisfy

$$(\frac{q^K}{B^{kK-2K+2}})^{1/(2K-1)} \ll q_0 \ll (\frac{q^K}{B^{kK-2K+2}})^{1/(2K-1)}$$

and

$$B(\frac{q}{B^kq_0})^{2^j/(2K-2)} \ll q_{k+1-j} \ll B(\frac{q}{B^kq_0})^{2^j/(2K-2)}, \quad (1 \le j \le k),$$

where $K = 2^k$. These constraints are compatible with $q = q_0q_1 \dots q_k$, and yield $q_i \gg 1$ for all i, providing that

$$q \gg B^{k-2+2/K}.$$

Under the above assumptions the theorem produces an estimate

$$\ll_{k,D,\varepsilon} q^{\varepsilon}\{B(\frac{q}{B^{k+2}})^{1/(4K-2)} + B^{1-1/K}(\frac{q}{B^{k+2}})^{-1/(4K-2)}\}, \tag{1.1}$$

which is non-trivial when

$$B^{k-2+2/K+\varepsilon'} \ll q \ll B^{k+2-\varepsilon'} \tag{1.2}$$

for some fixed $\varepsilon' > 0$. Thus, if q has suitably located factors, we may obtain a non-trivial result even when B is a small power of q.

The bound (1.1) should be compared with the well known 'k-th derivative estimate' for exponential sums, (with k replaced by $k+2$), see Titchmarsh [11; Theorem 5.13], for example.

2 Outline of the Method

We shall work with the set

$$\mathcal{A} = \{n + \sqrt[3]{2} : X < n \leq 2X\}$$

regarded as algebraic integers in $\mathbb{Q}(\sqrt[3]{2})$. These integers are composed solely of first degree prime ideals. Thus our goal is to show that a positive proportion of these integers have a prime ideal factor P with $N(P) \geq X^{1+\varpi}$. Here, and throughout the paper $N(\ldots)$ denotes the absolute norm on $\mathbb{Q}(\sqrt[3]{2})$. For any ideal I we define

$$\mathcal{A}_I = \{\alpha \in \mathcal{A} : I|\alpha\},$$

and we define

$$\rho(I) = \#\{n \pmod{N(I)} : n \equiv \sqrt[3]{2} \pmod{I}\}.$$

The following rather trivial result describes this function.

Lemma 1 *If $n \equiv \sqrt[3]{2} \pmod{I}$ is solvable with a rational integer n, then I is composed of first degree prime ideals only. Moreover I cannot be divisible by two distinct prime ideals of the same norm, nor by P_2^2 or P_3^2, where P_2 and P_3 are the primes above 2 and 3 respectively. In all other cases the congruence is solvable, and we have $\rho(I) = 1$. Moreover, if I is an ideal for which $\rho(I) = 1$, then for any $m \in \mathbb{Z}$, we have $I|m$ if and only if $N(I)|m$.*

The verification of this is left to the reader. We shall use Lemma 1 repeatedly in the course of our argument, without further comment. We should stress that the function $\rho(I)$ is not multiplicative. However we do have $\rho(IJ) = \rho(I)\rho(J)$ providing that $N(I)$ and $N(J)$ are coprime. It is clear that

$$\#\mathcal{A}_I = \frac{\rho(I)}{N(I)}X + O(1)$$

for any I, and we shall define

$$R_I = \#\mathcal{A}_I - \frac{\rho(I)}{N(I)}X,$$

so that $R_I = O(1)$.

We may factor the ideal $(n + \sqrt[3]{2})$ as

$$(n + \sqrt[3]{2}) = (\prod_{P^e || n+\sqrt[3]{2},\, N(P) \leq 3X} P^e)(\prod_{P^e || n+\sqrt[3]{2},\, N(P) > 3X} P^e).$$

Corresponding to this decomposition we write

$$\log(n^3 + 2) = \log N(n + \sqrt[3]{2}) = \log^{(1)}(n^3 + 2) + \log^{(2)}(n^3 + 2),$$

say, where

$$\log^{(1)}(n^3 + 2) = \sum_{P^e || n+\sqrt[3]{2},\, N(P) \leq 3X} \log N(P^e)$$

and

$$\log^{(2)}(n^3+2) = \sum_{P^e || n+\sqrt[3]{2},\, N(P)>3X} \log N(P^e).$$

Alternatively we may write

$$\log^{(1)}(n^3+2) = \sum_{I | n+\sqrt[3]{2},\, \Lambda(I)\le \log 3X} \Lambda(I).$$

Our principal task will be to construct a set $\mathcal{A}^{(1)} \subseteq \mathcal{A}$, with the property that $\log^{(1)}(n^3+2) \ge (1+\delta)\log X$ for $n \in \mathcal{A}^{(1)}$, for a certain constant $\delta > 0$. We shall also require that the cardinality X_1, say, of $\mathcal{A}^{(1)}$ satisfies $X_1 \gg X$. Now suppose that among the set $\mathcal{A}^{(2)} = \mathcal{A} \setminus \mathcal{A}^{(1)}$ there are precisely X_2 elements $n+\sqrt[3]{2}$ with $\log^{(1)}(n^3+2) \ge (1-\delta')\log X$, where δ' is to be chosen later. It then follows that

$$\sum_{n\in\mathcal{A}} \log^{(1)}(n^3+2) \ge X_1(1+\delta)\log X + X_2(1-\delta')\log X. \tag{2.1}$$

On the other hand, since $n^3+2 \le 9X^3$, we have

$$\begin{aligned}\sum_{n\in\mathcal{A}} \log^{(1)}(n^3+2) &= \sum_{N(I)\le 9X^3,\, \Lambda(I)\le \log 3X} \Lambda(I)\#\mathcal{A}_I \\ &= \sum_{N(I)\le 9X^3,\, \Lambda(I)\le \log 3X} \Lambda(I)\{X\frac{\rho(I)}{N(I)} + O(1)\}. \end{aligned} \tag{2.2}$$

However

$$\sum_{N(I)\le 9X^3,\, \Lambda(I)\le \log 3X} \Lambda(I)\frac{\rho(I)}{N(I)} = \sum_{N(P)\le 3X} \log N(P) \sum_{e:\, N(P^e)\le 9X^3} \frac{\rho(P^e)}{N(P^e)}.$$

It is clear that the total contribution from terms with exponent $e \ge 2$ is $O(1)$. The remaining part is therefore

$$\sum_{N(P)\le 3X} \frac{\log N(P)}{N(P)},$$

where the sum is for first degree primes only. By the Prime Ideal Theorem this is $\log X + O(1)$. We may also calculate that the error term in (2.2) is

$$\begin{aligned} &\ll \sum_{N(P)\le 3X} \log N(P) \sum_{e:\, N(P^e)\le 9X^3} 1 \\ &\ll \sum_{N(P)\le 3X} \log N(P)\frac{\log X}{\log N(P)} \\ &\ll X, \end{aligned}$$

by the Prime Ideal Theorem again. Thus (2.2) is $X\log X + O(X)$.

It therefore follows from (2.1) that

$$X_1(1+\delta) + X_2(1-\delta') \le X + O(\frac{X}{\log X}).$$

Now, if we set

$$\mathcal{A}^{(3)} = \{n + \sqrt[3]{2} \in \mathcal{A} : \log^{(1)}(n^3+2) < (1-\delta')\log X\}$$

and $X_3 = \#\mathcal{A}^{(3)} = X - X_1 - X_2$, we deduce that

$$X_1(1+\delta) + (X - X_1 - X_3)(1-\delta') \le X + O(\frac{X}{\log X}),$$

whence

$$X_3 \ge X_3(1-\delta') \ge X_1(\delta+\delta') - X\delta' + O(\frac{X}{\log X}).$$

We shall therefore choose

$$\delta' = \delta\frac{X_1}{X},$$

whence

$$X_3 \ge \delta(\frac{X_1}{X})^2 X + O(\frac{X}{\log X}).$$

Since

$$\sum_{I | n+\sqrt[3]{2}} \Lambda(I) = \log N(I) = \log(n^3+2) > 3\log X,$$

we deduce that

$$\log^{(2)}(n^3+2) = \log(n^3+2) - \log^{(1)}(n^3+2) > (2+\delta')\log X$$

for any $n + \sqrt[3]{2} \in \mathcal{A}^{(3)}$. Since $n^3 + 2 < (3X)^3$ for every $n + \sqrt[3]{2} \in \mathcal{A}$, the total multiplicity of all prime ideal factors P counted by $\log^{(2)}(n^3+2)$ can be at most 2. We then see that there must be a factor with

$$\log N(P) \ge \frac{(2+\delta')\log X}{2},$$

or equivalently $N(P) \ge X^{1+\delta'/2}$.

We now summarize our conclusions thus far.

Lemma 2 *Let α and δ be positive constants. Suppose that we have a set $\mathcal{A}^{(1)}$ of integers $n + \sqrt[3]{2}$ as above, with $\#\mathcal{A}^{(1)} \ge \alpha X$. Then the number of integers $n \in (X, 2X]$ for which $n^3 + 2$ has a prime factor $p \gg X^{1+\delta\alpha/2}$, is at least $(\delta\alpha^2 + o(1))X$.*

In order to construct elements $n + \sqrt[3]{2}$ of $\mathcal{A}^{(1)}$ we shall arrange that $n + \sqrt[3]{2}$ has an ideal factor $J = KL$ with

$$X^{1+\delta} < N(KL) \le X^{1+2\delta}, \tag{2.3}$$

and

$$X^{3\delta} < N(K) \le X^{4\delta}. \tag{2.4}$$

It will be convenient to impose the condition

$$\delta \in (0, \frac{1}{100}) \tag{2.5}$$

and to write

$$M = X^{(1+\delta)/3}, \quad N = X^{(1+2\delta)/3}. \tag{2.6}$$

For K, L as above we have

$$N(L) = \frac{N(J)}{N(K)} \leq X^{1-\delta}.$$

Since any factor P of J must divide either K or L, it follows that $N(P) \leq X$. Thus

$$\begin{aligned} \log^{(1)}(n^3+2) &= \sum_{I \mid n+\sqrt[3]{2},\ \Lambda(I) \leq \log 3X} \Lambda(I) \\ &\geq \sum_{I \mid J,\ \Lambda(I) \leq \log 3X} \Lambda(I) \\ &= \sum_{I \mid J} \Lambda(I) \\ &= \log N(J) \\ &\geq (1+\delta) \log X, \end{aligned}$$

as required.

We shall take K to run over the set $\mathcal{K}$ of first degree prime ideals satisfying (2.4). For each such K we shall let L run over a set $\mathcal{L}(K)$ to be described, subject to (2.3). However, if we were merely to count values of $n + \sqrt[3]{2}$ produced as multiples of the ideals J considered above, we would find that a given $n + \sqrt[3]{2}$ might occur many times. We avoid this difficulty by ensuring that L is composed only of prime ideals P with $N(P) > X^{\delta}$, say. To be more precise, we shall sieve L, from below, to level X^{δ}. Thus we take λ_d to be the Rosser weights for the lower bound sieve of dimension 1 and sieving limit 'D'$= X^{3\delta}$, as described by Iwaniec [7], for example. These are supported on the square-free integers $d \leq X^{3\delta}$ and have the properties that

$$|\lambda_d| \leq 1,$$

and

$$\sum_{d \mid n} \lambda_d \leq \begin{cases} 1, & n = 1, \\ 0, & n \geq 2. \end{cases} \tag{2.7}$$

Moreover, for any non-negative multiplicative function $g(d)$ satisfying $g(p) < p$ for all primes, and

$$\prod_{w \leq p < z} (1 - \frac{g(p)}{p})^{-1} \leq \frac{\log z}{\log w} \{1 + O(\frac{1}{\log w})\}$$

for all $z > w \geq 2$, we have

$$\sum_{d:\ p \mid d \Rightarrow p \leq X^{\delta}} g(d) \lambda_d d^{-1} \geq \{C_0 + o(1)\} \prod_{p \leq X^{\eta}} (1 - \frac{g(p)}{p}), \tag{2.8}$$

where

$$C_0 = \frac{2}{3} e^{\gamma} \log 2.$$

(Here we have 's'$= 3$ and '$f(s)$'$= C_0$, in the usual notation of sieve theory.)

We shall set

$$Q = \prod_{p<X^{\delta}} p,$$

the product being restricted to primes p which split in $\mathbb{Q}(\sqrt[3]{2})$. We then proceed to consider

$$\sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} (\sum_{d|Q,N(L)} \lambda_d)\mathcal{A}_{KL} = S,$$

say. In view of (2.7) we see that

$$\begin{aligned} S &\leq \sum_{K\in\mathcal{K}} \sum_{\substack{L\in\mathcal{L}(K)\\(N(L),Q)=1}} \mathcal{A}_{KL} \\ &= \sum_{n+\sqrt[3]{2}\in\mathcal{A}} \#\{(K,L) : K\in\mathcal{K},\ L\in\mathcal{L}(K),\ (N(L),Q)=1,\ KL|n+\sqrt[3]{2}\}. \end{aligned}$$

By construction, any $n+\sqrt[3]{2}$ which is counted with positive weight in the above sum will meet our requirements. However

$$n^3+2 \leq 9X^3 < X^{(1+[3\delta^{-1}])\delta},$$

for large enough X. We therefore see that $n+\sqrt[3]{2}$ can have at most $[3\delta^{-1}]$ prime ideal factors P, counted according to multiplicity, for which $N(P)\geq X^{\delta}$. Similarly, there can be at most $[\delta^{-1}]$ prime ideal factors P for which $N(P) > X^{3\delta}$. Moreover, if $\mathcal{A}_{KL}\neq\emptyset$ and $(N(L),Q)=1$ then L must be composed of first degree prime ideals P with $N(P)\geq X^{\delta}$. It follows that there are at most $[\delta^{-1}]$ possible choices for K, and at most $2^{[3/\delta]}$ possible choices for L, for any given choice of $n+\sqrt[3]{2}$. We have therefore produced at least $\delta 2^{-[3/\delta]}S$ suitable values of $n+\sqrt[3]{2}$.

On the other hand,

$$S = \sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} (\sum_{d|Q,N(L)} \lambda_d)\{X\frac{\rho(KL)}{N(KL)} + R_{KL}\} = XS_0 + S_1,$$

where

$$S_0 = \sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} (\sum_{d|Q,N(L)} \lambda_d)\frac{\rho(KL)}{N(KL)},$$

and

$$S_1 = \sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} (\sum_{d|Q,N(L)} \lambda_d)R_{KL}.$$

We shall regard these as a main term and a remainder term. In view of the analysis above we now have the following result.

Lemma 3 *Suppose that $S_1 = o(X)$. Then any constant α satisfying*

$$\alpha < \delta 2^{-[3/\delta]}S_0$$

will be acceptable in Lemma 2.

We remark that, with a little extra work, the exponential dependence on δ^{-1} can be replaced by a polynomial one. This improves the constant ϖ in Theorem 1 substantially.

We next turn our attention to the sum S_1. Here the following lemma, essentially due to Hooley [6], will play a crucial rôle.

Lemma 4 *Suppose a, b, c are integers, with a odd, and that $C = b^2 - ac$ and $D = a^2 + bc$ are both coprime to $q = a^3 - 2b^3$. Write $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ and $J = (\alpha)$. Then $(q, \alpha) = 1$. Moreover there is an integer k such that $n + \sqrt[3]{2} \in J$ if and only if $n \equiv k \pmod{N(J)}$. In particular we have $\rho(J) = 1$.*

Suppose further that N and H are positive integers. Let α run over a set of integers in $\mathbb{Q}(\sqrt[3]{2})$ with $a, b, c \ll N$, and suppose that $N(\alpha) \gg M^3$ and $q \gg M^3$ in each case, and that the ideals $J = (\alpha)$ are distinct. Let $\mathcal{J}$ be the set of ideals J produced in this way. Then, if $X' = X$ or $2X$ is suitably chosen, we have

$$\sum_{J \in \mathcal{J}} R_J \ll (\log H)(H^{-1} + HN^3M^{-6})\#\mathcal{J} + (\log H)^2 \sum_{n=1}^{H^2} \min(n^{-1}, Hn^{-2})|\sigma(n)|, \quad (2.9)$$

where

$$\sigma(n) = \sum_{J \in \mathcal{J}} e_q(-nab\overline{C}^{(q)}) e\Big(\frac{nX'}{N(\alpha)}\Big).$$

This will be proved in §3. The form of the hypotheses leads us to specify the set $\mathcal{L}(K)$ by taking $KL = (\alpha)$ where $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, with

$$2 \nmid a, \quad (2.10)$$

$$(b^2 - ac, a^3 - 2b^3) = 1, \quad (2.11)$$

$$(a^2 + bc, a^3 - 2b^3) = 1,$$

$$q = a^3 - 2b^3 \in \mathcal{Q},$$

and

$$(a, b, c) \in \mathcal{R},$$

where $\mathcal{Q} \subseteq \mathbb{N}$ is a set which will be specified in due course. Moreover the set $\mathcal{R} \subseteq \mathbb{R}^3$ is defined by the constraints

$$M^3 < N(\mathbf{x}) \leq N^3, \quad (2.12)$$

$$1 \leq \frac{x_1 + x_2\sqrt[3]{2} + x_3\sqrt[3]{4}}{N(\mathbf{x})^{1/3}} < \varepsilon_0, \quad (2.13)$$

and

$$x_1^3 - 2x_2^3 \geq M^3.$$

Here $\mathbf{x} = (x_1, x_2, x_3)$ and

$$N(\mathbf{x}) = x_1^3 + 2x_2^3 + 4x_3^3 - 6x_1x_2x_3,$$

while $\varepsilon_0 = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ is the fundamental unit of $\mathbb{Q}(\sqrt[3]{2})$. Conditions (2.12) and (2.13) then yield $a, b, c \ll N$. Moreover (2.13) will ensure that the ideals (α) are distinct. We also note that (2.11) and (2.10) yield

$$(a, b) = (2ab, q) = 1. \tag{2.14}$$

We now return to the remainder term S_1. Here we shall apply Theorem 2 to estimate the sums $\sigma(n)$ occuring in Lemma 4. The necessary cancellation will come from the variable c, which is essentially of order $q^{1/3}$. Thus the case $k = 1$ of Theorem 2 is not quite sufficient to give a non-trivial bound, as the condition (1.2) shows. We therefore take $k = 2$, which will produce a useable estimate providing the factors q_i are sufficiently close to their theoretical optimal values. We shall therefore define the set $\mathcal{Q}$ by the conditions

$$q \text{ is square-free,} \tag{2.15}$$

$$(q, 6) = 1, \tag{2.16}$$

$$\exists q_1 q_2 | q \text{ with } N^{5/7} < q_1 \leq N^{5/7+\delta}, \text{ and } N^{6/7} < q_2 \leq N^{6/7+\delta}. \tag{2.17}$$

Note that (2.15) implies that that $(a, b) = 1$, and that (2.16) implies (2.10). Under the above assumptions we may estimate S_1 via the following result, which will be proved in §5.

Lemma 5 *We have $S_1 = o(X)$ providing that $\delta \leq 1/321$.*

It remains to estimate S_0 from below. The first stage in this process is given by the following result.

Lemma 6 *Define*

$$I(a, b) = \int_{(a,b,t)\in\mathcal{R}} N(a, b, t)^{-1} dt$$

and

$$g(p) = \#\{P : N(P) = p\}.$$

Then

$$S_0 \geq 2\{C_0 + o(1)\}(\log 4/3) \prod_{p<X^\delta} (1 - g(p)/p) \sum_{a,b:\, q\in\mathcal{Q}} I(a, b)h(q) + o(1),$$

where

$$h(q) = \prod_{p|q} \left(\frac{1 - 2/p}{1 - g(p)/p}\right),$$

if q is square-free and coprime to 6, and $h(q) = 0$ otherwise.

This will be proved in §6.

Our second major task will be to construct suitably many elements of $\mathcal{Q}$. It will suffice to consider prime values of q_1 and q_2. Define multiplicative functions $l(m)$ and $\nu(m)$ as follows. We put $l(p^e) = 0$ for $e \geq 3$, and

$$l(3) = -1, \quad l(3^2) = 0, \tag{2.18}$$

$$l(p) = \frac{g(p) - 2}{p - g(p)}, \quad l(p^2) = -\frac{p - 2}{p - g(p)}, \quad (p \neq 3). \tag{2.19}$$

Moreover we take

$$\nu(p^e) = \frac{g(p)}{1+p^{-1}}.$$

We then have the following result.

Lemma 7 *Let $A, B \ll N$ and write*

$$C(m) = \sum_{\substack{A<a\le A+M,\, B<b\le B+M \\ m|q}} h(q). \tag{2.20}$$

Suppose that

$$(0,0) \notin (A, A+M] \times (B, B+M]. \tag{2.21}$$

Then if

$$C_1 = \frac{6}{\pi^2}\sum_{d=1}^{\infty} l(d)\frac{\nu(d)}{d},$$

we have

$$\sum_{q_1,q_2} |C(q_1q_2) - C_1M^2\frac{\nu(q_1)\nu(q_2)}{q_1q_2}| \ll M^2N^{-\delta},$$

the sum being over prime values of q_1, q_2 in the ranges (2.17).

It is now straightforward to prove the following lower bound for S_0.

Lemma 8 *Let*

$$C_2 = 2C_0(\log\frac{4}{3})\frac{1}{3}C_1\frac{\pi}{12\sqrt{3}}(\log\varepsilon_0).$$

Then

$$S_0 \ge \{C_2 + o(1)\}\delta L(\delta)(\log X)\prod_{p<X^\delta}(1-\frac{g(p)}{p}),$$

where

$$L(\delta) = (\log(1+7\delta/5))(\log(1+7\delta/6)).$$

Finally we need a result concerning the product that appears here.

Lemma 9 *We have*

$$\prod_{p\le x}(1-\frac{g(p)}{p}) \sim \frac{C_3}{\log x},$$

where

$$C_3 = \frac{\sqrt{27}}{e^\gamma\pi\log\varepsilon_0}\prod_p\{(1-\frac{g(p)}{p})\prod_{N(P)=p}(1-\frac{1}{N(P)})^{-1}\}.$$

It follows from Lemmas 8 and 9 that

$$S_0 \ge C_2C_3L(\delta) + o(1).$$

In view of the definitions of the various constants we may calculate that

$$C_2C_3 = \frac{(\log 2)(\log 4/3)}{3\pi^2}\prod_{p\ge5}k(p),$$

where

$$k(p) = \begin{cases} (1-p^{-3})^{-1}, & g(p) = 0, \\ 1-(p+1)^{-2}, & g(p) = 1, \\ 1-\frac{3p^2-4p-1}{(p-1)^3(p+1)}, & g(p) = 3. \end{cases}$$

This yields

$$\prod_{p \geq 5} k(p) \geq 0.91,$$

and hence

$$C_2 C_3 \geq 6.1 \times 10^{-3}.$$

If we now choose $\delta = 1/321$, as suggested by Lemma 5, we find that

$$S_0 \geq C_2 C_3 L(\delta) + o(1) \geq 9.2 \times 10^{-8},$$

for large enough X. According to Lemma 3 we may choose

$$\alpha = 10^{-300} < 9.2 \times 10^{-8} \times \frac{1}{321} 2^{-963},$$

Theorem 1 then follows from Lemma 2, with

$$\varpi = 10^{-303} < \delta\alpha/2,$$

as claimed.

3 Proof of Lemma 4

We begin the proof by establishing the following coprimality conditions. Let

$$A = a^2 - 2bc, \quad B = 2c^2 - ab.$$

Then we have

$$(N(\alpha), q) = 1, \tag{3.1}$$

$$(A, C) = 1, \tag{3.2}$$

and

$$(N(\alpha), C) = 1. \tag{3.3}$$

It clearly follows from (3.1) that $(q, \alpha) = 1$, as required for the lemma. We note at the outset that q is odd, since a is. Then, to prove (3.1), we have only to use the identity

$$4C^2 D = a^2 b N(\alpha) + \{4ac^2 - 2b^2 c - a^2 b\} q$$

and recall that $(2CD, q) = 1$. To prove (3.2) we note that

$$q = aA - 2bC,$$

whence $(A, C) | (q, C) = 1$, by hypothesis. Finally, to prove (3.3) we observe that

$$aN(\alpha) = A^2 - 2BC.$$

This shows that $(N(\alpha), C) | A^2$. Thus (3.2) implies (3.3).

Having dealt with these preliminary assertions, we observe that

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \equiv 0 \pmod{J}$$

and

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})\sqrt[3]{2} = 2c + a\sqrt[3]{2} + b\sqrt[3]{4} \equiv 0 \pmod{J}.$$

On eliminating $\sqrt[3]{4}$ we obtain $C\sqrt[3]{2} \equiv B \pmod{J}$. Since $(C, J) = 1$, by (3.3), we see that $\rho(J) = 1$ and that $n + \sqrt[3]{2} \in J$ if and only if $Cn + B \in J$. By Lemma 1 this last condition is equivalent to $N(J)|Cn + B$. This proves the first assertion of the lemma with

$$k \equiv -B\overline{C}^{(N(\alpha))} \pmod{N(\alpha)},$$

where

$$C\overline{C}^{(N(\alpha))} \equiv 1 \pmod{N(\alpha)}.$$

Note that C does indeed have an inverse modulo $N(\alpha)$, in view of (3.3).

We now examine $\#\mathcal{A}_J$. It will be convenient to write k_J for the value of k corresponding to the ideal J, so that

$$k_J \equiv -B\overline{C}^{(N(\alpha))} \pmod{N(\alpha)}.$$

According to what we have proved so far,

$$\begin{aligned} \#\mathcal{A}_J &= \#\{n : X < n \le 2X,\, n \equiv k \pmod{N(J)}\} \\ &= \#\{m : \frac{X-k}{N(J)} < m \le \frac{2X-k}{N(J)}\} \\ &= \frac{X}{N(J)} + \psi(\frac{X-k}{N(J)}) - \psi(\frac{2X-k}{N(J)}), \end{aligned}$$

where $\psi(t) = t - [t] - \frac{1}{2}$. Now

$$\psi(t) = -\sum_{n \le H} \frac{\sin(2\pi nt)}{\pi n} + O(\min\{1\,,\, (H||t||)^{-1}\}). \tag{3.4}$$

The sum on the left contributes to (2.9) a total

$$\begin{aligned} &\ll \sum_{n \le H} n^{-1} |\sum_{J \in \mathcal{J}} \{\sin(n\frac{2X - k_J}{N(J)}) - \sin(n\frac{X - k_J}{N(J)})\}| \\ &\ll \sum_{n \le H} n^{-1} |\Sigma(n)|, \end{aligned}$$

for $X' = X$ or $2X$, where

$$\Sigma(n) = \sum_{J \in \mathcal{J}} e_{N(J)}(n(X' - k_J)).$$

Since

$$\min\{1\,,\, (H||t||)^{-1}\} = \sum_{-\infty}^{\infty} c_n e(nt)$$

with

$$c_n \ll \min\{\frac{\log H}{H}\,,\, \frac{H}{n^2}\},$$

we find that the error term in (3.4) contributes to (2.9) a total

$$\begin{aligned} &\ll \sum_{J\in\mathcal{J}} \min\{1\,,\, \frac{1}{H||(X'-k_J)/N(J)||}\} \\ &= \sum_{J\in\mathcal{J}} \sum_{-\infty}^{\infty} c_n e_{N(J)}(n(X'-k_J)) \\ &= \sum_{-\infty}^{\infty} c_n \sum_{J\in\mathcal{J}} e_{N(J)}(n(X'-k_J)) \\ &\ll \sum_{-\infty}^{\infty} \min\{\frac{\log H}{H}\,,\, \frac{H}{n^2}\}|\Sigma(n)|. \end{aligned}$$

We may therefore conclude that

$$\begin{aligned} \sum_{J\in\mathcal{J}} R_J &\ll (\log H)H^{-1}\#\mathcal{J} + (\log H)\sum_{n=1}^{\infty} \min(n^{-1}\,,\, Hn^{-2})|\Sigma(n)| \\ &\ll (\log H)H^{-1}\#\mathcal{J} + (\log H)\sum_{n=1}^{H^2} \min(n^{-1}\,,\, Hn^{-2})|\Sigma(n)|, \end{aligned}$$

in view of the trivial bound $\Sigma(n) \ll \#\mathcal{J}$.

In order to handle the sum $\Sigma(n)$ more effectively, we shall show that

$$\frac{k_J}{N(J)} \equiv \frac{ab\overline{C}^{(q)}}{q} + \frac{2a^2c + 4bc^2 - 4ab^2}{qN(J)} \pmod 1. \tag{3.5}$$

In order to verify this we note that $N(J)$ and q are coprime, by (3.1). Thus it suffices to show that

$$-abN(\alpha)\overline{C}^{(q)} \equiv 2a^2c + 4bc^2 - 4ab^2 \pmod q$$

and

$$k_J q \equiv 2a^2c + 4bc^2 - 4ab^2 \pmod{N(J)}.$$

However, the identity

$$C(2a^2c + 4bc^2 - 4ab^2) = -abN(\alpha) - Bq$$

shows that

$$\begin{aligned} -abN(\alpha)\overline{C}^{(q)} &\equiv C\overline{C}^{(q)}(2a^2c + 4bc^2 - 4ab^2) \\ &\equiv 2a^2c + 4bc^2 - 4ab^2 \pmod q, \end{aligned}$$

and also that

$$\begin{aligned} k_J q &\equiv -B\overline{C}^{(N(\alpha))} q \\ &\equiv C\overline{C}^{(N(\alpha))}(2a^2c + 4bc^2 - 4ab^2) \\ &\equiv 2a^2c + 4bc^2 - 4ab^2 \pmod{N(J)}, \end{aligned}$$

as required. This completes the proof of (3.5).

It now follows from (3.5) that

$$e_{N(J)}(n(X'-k_J)) = e_q(-nab\overline{C}^{(q)})e(\frac{nX'}{N(\alpha)}) + O(nN^3M^{-6}),$$

so that

$$\Sigma(n) = \sigma(n) + O(nN^3M^{-6}\#\mathcal{J}).$$

The error term makes a contribution $O(H(\log H)^2N^3M^{-6}\#\mathcal{J})$ to (2.9), and the final assertion of Lemma 4 follows.

4 Preliminary Transformation of the Sums S_0 and S_1

The initial stages in our treatment of the sums S_0 and S_1 are the same, and will be described in this section.

We recall that

$$S_0 = \sum_{K\in\mathcal{K}}\sum_{L\in\mathcal{L}(K)}(\sum_{d|Q,N(L)}\lambda_d)\frac{\rho(KL)}{N(KL)}$$

and

$$S_1 = \sum_{K\in\mathcal{K}}\sum_{L\in\mathcal{L}(K)}(\sum_{d|Q,N(L)}\lambda_d)R_{N(KL)}.$$

According to Lemma 4, we will have $\rho(KL) = 1$ for every $L \in \mathcal{L}(K)$. We may therefore introduce a factor $\rho(KL)$ into the sum S_1. Since $\rho(KL) = 1$ we see that L is composed of first degree prime ideals. Let

$$R = \prod_{2<N(P)<X^\delta} P,$$

the product being restricted to first degree primes. We proceed to show that we may take d to run over all square-free values of $N(A)$, where $A|R, L$. To prove this we let $(L, d) = A$, say. Then $A|Q$, so that A must be composed of first degree prime ideals P with $N(P) < x^\delta$. We also have $(2, KL) = 1$ by (2.10), whence $(2, A) = 1$. Since $\rho(KL) = 1$ we have $\rho(A) = 1$. Thus A cannot have two distinct prime factors of the same norm, nor can P_3^2 divide A, where P_3 is the prime ideal above 3. Moreover, since we may assume d to be square-free, we cannot have $P^2|d$ for any $P \neq P_3$, either. Thus A must divide R, and $N(A)$ must be square-free. Since $A|d$ we have $N(A)|d^3$, whence $N(A)|d$. On the other hand if p is a prime factor of d, then $p|N(L)$, whence L must have a prime ideal factor P of norm p. Then $P|L, d$ so that $P|A$ and $p|N(A)$. It follows that $d|N(A)$, and hence that $N(A) = d$. Thus each value of d arises as $N(A)$. Conversely we note that if $A|R$ and $N(A)$ is square-free, then $A|L$ implies $N(A)|Q, N(L)$. Hence each possible A produces an admissible value $d = N(A)$. This establishes the result claimed above.

It now follows that

$$S_0 = \sum_{K\in\mathcal{K}}\sum_{L\in\mathcal{L}(K)}(\sum_{A|R,L}\lambda_{N(A)})\frac{\rho(KL)}{N(KL)}$$

and

$$S_1 = \sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} \Big(\sum_{A|R,L} \lambda_{N(A)}\Big)\rho(KL)R_{N(KL)}.$$

We see from the condition (2.4) for $\mathcal{K}$ and the fact that λ_d is supported on $d \le X^{3\delta}$ that K and A can be taken to be coprime. For every $L \in \mathcal{L}(K)$ we have $\rho(KL) = 1$ and $(KL, q) = 1$, by Lemma 4. We may therefore write

$$S_0 = \sum_{K\in\mathcal{K}} \sum_{A|R} \lambda_{N(A)}\rho(KA) \sum_{L\in\mathcal{L}(K),\, A|L,\, (KA,q)=1} N(KL)^{-1}$$

and

$$S_1 = \sum_{K\in\mathcal{K}} \sum_{A|R} \lambda_{N(A)}\rho(KA) \sum_{L\in\mathcal{L}(K),\, A|L,\, (KA,q)=1} R_{N(KL)}.$$

We proceed to investigate the innermost sums above, by putting

$$KL = (a + b\sqrt[3]{2} + c\sqrt[3]{4})$$

and summing over c for fixed a, b. The conditions

$$M^3 \le N(\alpha) < N^3, \quad 1 \le \frac{\alpha}{N(\alpha)^{1/3}} < \varepsilon_0,$$

then define for c a set $\mathcal{C} = \mathcal{C}(a, b)$ which is a disjoint union of at most 3 intervals. If we write

$$u = x_1 + x_2\sqrt[3]{2} + x_3\sqrt[3]{4}, \quad v = x_1 + x_2\omega\sqrt[3]{2} + x_3\omega^2\sqrt[3]{4},$$

where $\omega = (-1 + \sqrt{-3})/2$, then $N(\mathbf{x}) = u|v|^2$, and (2.13) implies that $v \ll N(\mathbf{x})^{1/3}$. Since we also have $u \ll N(\mathbf{x})^{1/3}$ and $\overline{v} \ll N(\mathbf{x})^{1/3}$ we may conclude that

$$x_1, x_2, x_3 \ll N(\mathbf{x})^{1/3} \quad (\mathbf{x} \in \mathcal{R}). \tag{4.1}$$

Thus

$$a, b, c \ll N(\alpha)^{1/3} \ll N.$$

We introduce the coprimality conditions

$$(b^2 - ac, q) = 1, \quad (a^2 + bc, q) = 1,$$

via sums involving the Möbius function, to deduce that

$$\sum_{L\in\mathcal{L}(K),\, A|L,\, (A,q)=1} N(KL)^{-1} = \sum_{\substack{a,b \\ q\in\mathcal{Q},\, (KA,q)=1}} \sum_{r,s|q} \mu(r)\mu(s) \sum_{c} N(\alpha)^{-1}$$

and

$$\sum_{L\in\mathcal{L}(K),\, A|L,\, (A,q)=1} NR_{KL} = \sum_{\substack{a,b \\ q\in\mathcal{Q},\, (KA,q)=1}} \sum_{r,s|q} \mu(r)\mu(s) \sum_{c} R_{(\alpha)},$$

where the sum over c is subject to

$$c \in \mathcal{C}, \quad KA|a + b\sqrt[3]{2} + c\sqrt[3]{4}, \quad r|b^2 - ac, \quad s|a^2 + bc. \tag{4.2}$$

Since we may assume that $\rho(KA) = 1$ it follows that there is a rational integer j, say, for which $\sqrt[3]{2} \equiv j \pmod{KA}$. The condition $KA|a+b\sqrt[3]{2}+c\sqrt[3]{4}$ is therefore equivalent to a congruence of the form $c \equiv c_1(a, b, KA) \pmod{KA}$, for some rational integer $c_1(a, b, KA)$, and this itself is equivalent to

$$c \equiv c_1(a, b, KA) \pmod{N(KA)}.$$

To handle the conditions $r|b^2 - ac$ and $s|a^2 + bc$ we begin by observing that if r and s have a common prime factor p, say, then

$$b^3 = b.b^2 \equiv b.ac = a.bc \equiv -a.a^2 = -a^3 \pmod{p}.$$

However $p|q$, since $r|q$, whence $p|a^3 - 2b^3$. It follows that $p|3b$, which is impossible, since $(q, 3b) = 1$ by (2.14) and (2.16). We may therefore assume that $(r, s) = 1$ in (4.2). Moreover we will have $(r, a) = (s, b) = 1$, since $(q, ab) = 1$, by (2.14). We then see that the conditions $r|b^2 - ac$ and $s|a^2 + bc$ are equivalent to a congruence

$$c \equiv c_2(a, b, r, s) \pmod{rs}$$

for a suitable rational integer $c_2(a, b, r, s)$. Since we have $(KA, q) = 1$ we may now replace (4.2) by

$$c \in \mathcal{C}, \quad c \equiv c_3(a, b, KA, r, s) \pmod{rsN(KA)}. \tag{4.3}$$

We therefore conclude that

$$S_0 = \sum_{K\in\mathcal{K}} \sum_{A|R} \lambda_{N(A)}\rho(KA) \sum_{\substack{a,b \\ q\in\mathcal{Q},\,(KA,q)=1}} \sum_{\substack{r,s|q \\ (r,s)=1}} \mu(r)\mu(s) \sum_{c} N(\alpha)^{-1} \tag{4.4}$$

and

$$S_1 = \sum_{K\in\mathcal{K}} \sum_{A|R} \lambda_{N(A)}\rho(KA) \sum_{\substack{a,b \\ q\in\mathcal{Q},\,(KA,q)=1}} \sum_{\substack{r,s|q \\ (r,s)=1}} \mu(r)\mu(s) \sum_{c} R_{(\alpha)},$$

with c running over the set given by (4.3).

5 The Remainder Sum S_1

It follows from our work in the previous section that

$$S_1 \ll \sum_{K\in\mathcal{K}} \sum_{N(A)\le X^{3\delta}} \sum_{a,b\ll N} \sum_{r,s|q} |\sum_{c} R_{(\alpha)}|, \tag{5.1}$$

where the sum over c is subject to (4.3).

We are now ready to apply Lemma 4, taking $\mathcal{J}$ to run over integers α for which a and b are fixed, and c runs over the set (4.3). We shall write

$$c = c_3(a, b, KA, r, s) + mrsN(KA),$$

so that m runs over a union of at most 3 intervals, whose total length is $O(1+N/rsN(KA))$. In order to put $\sigma(n)$ into a shape suitable for Theorem 2, we shall write

$$g(X) = b^2 - a\{c_3(a,b,KA,r,s) + XrsN(KA)\} = c_4 - arsN(KA)X,$$

where

$$c_4 = c_4(a,b,KA,r,s) = b^2 - ac_3(a,b,KA,r,s).$$

Clearly we may exclude values of r, s, A and K for which c_4 is not coprime to rs. Then $(C,q) = 1$ if and only if $(g(m), q') = 1$, where $q' = q(rs)^{-1}$. Moreover

$$\overline{C}^{(q)} \equiv \overline{g(m)}^{(q')} \equiv rs\overline{rs}^{(q')}\overline{g(m)}^{(q')} \pmod{q'},$$

on noting that $(rs, q') = 1$, by (2.15). We also have

$$\overline{C}^{(q)} \equiv \overline{c_4}^{(rs)} \equiv q'\overline{q'}^{(rs)}\overline{c_4}^{(rs)} \pmod{rs},$$

whence

$$\overline{C}^{(q)} \equiv rs\overline{rs}^{(q')}\overline{g(m)}^{(q')} + q'c_5 \pmod{q},$$

with

$$c_5 = \overline{q'c_4}^{(rs)}.$$

If we now set

$$w = -nab\overline{rs}^{(q')}$$

we may conclude that

$$\sigma(n) = e_{rs}(-nabc_5)\sum_m e_{q'}(w\overline{g(m)}^{(q')})e(nX'/N(\alpha)).$$

We now wish to remove the factor $e(nX'/N(\alpha))$, using partial summation. It follows from (4.1) that

$$\nabla N(\mathbf{x})^{-1} \ll N(\mathbf{x})^{-4/3} \quad (\mathbf{x} \in \mathcal{R}), \tag{5.2}$$

whence

$$\frac{d}{dt}N(a + b\sqrt[3]{2} + t\sqrt[3]{4})^{-1} \ll N(\alpha)^{-4/3} \ll M^{-4}, \quad (t \in \mathcal{C}). \tag{5.3}$$

This estimate allows us to conclude, by partial summation, that

$$\sigma(n) \ll (1 + nXNM^{-4})|\sum_{B'<m\le B'+B} e_{q'}(w\overline{g(m)}^{(q')})|,$$

for some integers B' and B with $B \ll 1 + N/rsN(AK)$. Since $XNM^{-4} \le 1$, by (2.6), this implies that

$$\sigma(n) \ll n|\sum_{B'<m\le B'+B} e_{q'}(w\overline{g(m)}^{(q')})|.$$

Theorem 2 may now be applied with $k = 2$ and $D = 1$. We have $p > 4$ for all $p|q'$, by (2.16). Since $f(X) = 1$ and $g(X)$ is non-constant modulo any

prime factor p of q', the hypotheses of the theorem are satisfied. We shall take $q_1' = q_1/(rs, q_1)$ and $q_2' = q_2/(rs, q_2)$, whence $q_1'q_2'|q'$. We may then deduce that

$$\sigma(n) \ll nX^{\varepsilon}\{Bq_0^{-1/8}(q_0, w)^{1/8} + B^{3/4}q_0^{1/8} + B^{3/4}q_1^{1/4} + B^{1/2}q_2^{1/2}\},$$

with $q_0 = q'/q_1'q_2'$. We recall that $(q, ab) = 1$, by (2.14), whence $(q_0, w)^{1/8} \leq (q, n)$. Moreover, the inequalities (2.17) yield

$$q_0 = \frac{q}{q_1q_2}\frac{(rs, q_1)(rs, q_2)}{rs} \leq \frac{q}{q_1q_2} \ll N^{10/7}$$

and

$$\begin{aligned} q_0 &\geq \frac{q}{q_1q_2}\frac{1}{rs} \\ &\gg M^3N^{-11/7-2\delta}(rs)^{-1} \\ &= N^3X^{-\delta}N^{-11/7-2\delta}(rs)^{-1} \\ &\geq N^3(N^3)^{-\delta}N^{-11/7-2\delta}(rs)^{-1} \\ &= N^{10/7-5\delta}(rs)^{-1}. \end{aligned}$$

since $M^3 \ll q \ll N^3$. This leads to the bound

$$\sigma(n) \ll nX^{\varepsilon}\{BN^{-5/28+5\delta/8}(rs)^{1/8} + B^{3/4}N^{5/28+\delta/4} + B^{1/2}N^{3/7+\delta/2}\}(q, n).$$

However

$$\begin{aligned} B^{1/2}(rs)^{1/8} &\ll (1 + \frac{N}{rs})^{1/2}(rs)^{1/8} \\ &\ll q^{1/8} + N^{1/2} \\ &\ll N^{1/2}, \end{aligned}$$

since $q \ll N^3$. It therefore follows that

$$\sigma(n) \ll nX^{\varepsilon}B^{1/2}N^{3/7+\delta/2}(q, n).$$

We feed this bound for $\sigma(n)$ into Lemma 4, assuming that $H \leq X$, and noting by (2.6) that $N^3M^{-6} = X^{-1}$. This produces

$$\sum_c R_{(\alpha)} \ll X^{\varepsilon}(H^{-1} + HX^{-1})B + X^{2\varepsilon}B^{1/2}N^{3/7+\delta/2}\sum_{n=1}^{H^2}\min(1\,,\,\frac{H}{n})(q, n).$$

Since

$$\sum_{n\leq x}(q, n) \leq \sum_{k|q}k\#\{n \leq x : k|n\} \leq xd(q),$$

we have

$$\sum_{n=1}^{H^2}\min(1\,,\,Hn^{-1})(q, n) \ll HX^{\varepsilon}.$$

This leads to

$$\sum_c R_{(\alpha)} \ll \{(H^{-1} + HX^{-1})B + HB^{1/2}N^{3/7+\delta/2}\}X^{3\varepsilon}.$$

We therefore choose

$$H = 1 + [B^{1/4}N^{-3/14-\delta/4}].$$

Since this yields $H \ll N^{1/28} \ll X^{1/2}$, we deduce that

$$\sum_c R_{(\alpha)} \ll \{B^{3/4}N^{3/14+\delta/4} + B^{1/2}N^{3/7+\delta/2}\}X^{3\varepsilon}.$$

We insert this bound into (5.1), to deduce that

$$S_1 \ll X^{3\varepsilon} \sum_{K\in\mathcal{K}} \sum_{N(A)\le X^{3\delta}} \sum_{a,b\ll N} \sum_{r,s|q} \{B^{3/4}N^{3/14+\delta/4} + B^{1/2}N^{3/7+\delta/2}\}.$$

However

$$\sum_{r,s|q} B^{\phi} \ll d(q)^2(1 + \frac{N}{N(KA)})^{\phi}$$

for $\phi = 1/2$ or $3/4$, and

$$\sum_{K\in\mathcal{K}} \sum_{N(A)\le X^{3\delta}} (1 + \frac{N}{N(KA)})^{\phi} \ll X^{7\delta}(\frac{N}{X^{7\delta}})^{\phi},$$

by (2.4) and (2.5). We therefore have

$$\begin{aligned} S_1 &\ll X^{4\varepsilon}N^2X^{7\delta}\{N^{3/14+\delta/4}(\frac{N}{X^{7\delta}})^{3/4} + N^{3/7+\delta/2}(\frac{N}{X^{7\delta}})^{1/2}\} \\ &= X^{4\varepsilon}N^3\{N^{3/14+\delta/4}(\frac{N}{X^{7\delta}})^{-1/4} + N^{3/7+\delta/2}(\frac{N}{X^{7\delta}})^{-1/2}\}. \end{aligned}$$

Thus we will have $S_1 \ll X^{1-\varepsilon}$, for example, providing that

$$N^{3/7+\delta/2}(\frac{N}{X^{7\delta}})^{-1/2} \ll X^{-10\varepsilon-4\delta}.$$

This latter condition is equivalent to

$$X^{15\delta/2+10\varepsilon} \ll N^{1/14-\delta/2},$$

or

$$15\delta/2 + 10\varepsilon \le (1/14 - \delta/2)(\frac{1+2\delta}{3}).$$

This is satisfied for $\delta \le 1/321$, if ε is small enough, and Lemma 5 follows.

6 The Main Term, S_0

In this section we shall prove Lemma 6, which estimates

$$S_0 = \sum_{K\in\mathcal{K}} \sum_{L\in\mathcal{L}(K)} (\sum_{d|Q,N(L)} \lambda_d) \frac{\rho(KL)}{N(KL)}.$$

According to (4.4) we have

$$S_0 = \sum_{K\in\mathcal{K}} \sum_{A|R} \lambda_{N(A)}\rho(KA) \sum_{\substack{a,b \\ q\in\mathcal{Q},\,(KA,q)=1}} \sum_{\substack{r,s|q \\ (r,s)=1}} \mu(r)\mu(s) \sum_c N(\alpha)^{-1}.$$

We may now use partial summation, coupled with the bounds (2.12) and (5.3), to compute that

$$\sum_{c\in\mathcal{C},\, c\equiv c_3 \pmod{rsN(KA)}} N(\alpha)^{-1} = \frac{1}{rsN(KA)} I(a,b) + O(NM^{-4}),$$

where

$$I(a,b) = \int_{(a,b,t)\in\mathcal{R}} N(a,b,t)^{-1} dt,$$

as in the statement of Lemma 6. If we write

$$\sum_{r,s|q,\ (r,s)=1} \frac{\mu(r)\mu(s)}{rs} = \prod_{p|q}(1-2/p) = f(q),$$

say, it follows that

$$\begin{aligned} S_0 \quad = \quad & \sum_{K\in\mathcal{K}} \frac{\rho(K)}{N(K)} \sum_{a,b:\, q\in\mathcal{Q},\, (K,q)=1} f(q) I(a,b) \sum_{A|R,\, (A,q)=1} \lambda_{N(A)} \frac{\rho(A)}{N(A)} \\ & + O(N^{3+\varepsilon} M^{-4} \sum_{K\in\mathcal{K},\, A|R} |\lambda_{N(A)}|), \end{aligned}$$

since

$$\sum_{a,b,r,s} 1 \ll N^{2+\varepsilon}$$

for any fixed $\varepsilon > 0$. Since $N(K) \le X^{4\delta}$ and $N(A) \le X^{3\delta}$ we find that the error term is

$$\ll N^{3+\varepsilon} M^{-4} X^{7\delta} \ll X^{-1/3+23\delta/3+\varepsilon}.$$

On taking ε sufficiently small, we conclude, in view of (2.5), that

$$S_0 = \sum_{a,b:\, q\in\mathcal{Q}} f(q) I(a,b) \sigma_1(q) \sigma_2(q) + o(1). \tag{6.1}$$

Here we have defined

$$\sigma_1(q) = \sum_{K\in\mathcal{K},\, (K,q)=1} \frac{\rho(K)}{N(K)}, \tag{6.2}$$

and

$$\sigma_2(q) = \sum_{A|R,\, (A,q)=1} \lambda_{N(A)} \frac{\rho(A)}{N(A)}.$$

We proceed to examine the sum $\sigma_1(q)$. If we drop the condition $(K,q) = 1$ the resulting error is at most

$$\sum_{K\in\mathcal{K},\, K|q} N(K)^{-1} \le X^{-3\delta+\varepsilon},$$

since K runs over primes in the range (2.4). Indeed, if $K \in \mathcal{K}$ and $\rho(K) = 1$, then $N(K)$ is a prime p in the range $(X^{3\delta}, X^{4\delta}]$. Conversely, for such a prime p, if $N(K) = p$ then $K \in \mathcal{K}$ and $\rho(K) = 1$. It follows that

$$\sum_{K\in\mathcal{K}} \frac{\rho(K)}{N(K)} = \sum_{X^{3\delta} < p \le X^{4\delta}} g(p)/p,$$

where

$$g(p) = \#\{P : N(P) = p\}.$$

By the Prime Ideal Theorem we have

$$\sum_{n\le x} g(p) = \{1 + O(\frac{1}{\log x})\}\frac{x}{\log x},$$

since prime ideals of degree 2 or more make a negligible contribution. We therefore conclude that

$$\sum_{K\in\mathcal{K}} \frac{\rho(K)}{N(K)} = \log\log X^{4\delta} - \log\log X^{3\delta} + o(1) = \log(4/3) + o(1). \tag{6.3}$$

Thus (6.2) is asymptotically $\log(4/3)$.

We turn lastly to the sum

$$\sigma_2(q) = \sum_{A|R,\,(A,q)=1} \lambda_{N(A)}\frac{\rho(A)}{N(A)}.$$

If we set $N(A) = d$ then we will find that d is square-free with $d|Q$ and $(d, 2q) = 1$. Moreover, for such d, if $N(A) = d$, then $A|R, (A, q) = 1$ and $\rho(A) = 1$. It follows that

$$\sigma_2(q) = \sum_{d|Q} \lambda_d g_q(d)/d,$$

where $g_q(d)$ is the multiplicative function defined by taking $g_q(p) = 0$ for $p|2q$, and

$$g_q(p) = \#\{P : N(P) = p\}$$

otherwise. Clearly $g_q(p) \le g(p)$, whence

$$\prod_{w\le p<z} (1 - \frac{g_q(p)}{p})^{-1} \le \prod_{w\le p<z} (1 - \frac{g(p)}{p})^{-1}$$

for $z > w \ge 2$. Moreover

$$\begin{aligned}\sum_{w\le p<z} \frac{g(p)}{p} &= \sum_{w\le N(P)<z} N(P)^{-1} + O(w^{-1/2}) \\ &= \log\log z - \log\log w + O((\log w)^{-1}),\end{aligned}$$

by the Prime Ideal Theorem, so that

$$\prod_{w\le p<z} (1 - \frac{g(p)}{p})^{-1} \le \frac{\log z}{\log w}\{1 + O(\frac{1}{\log w})\}.$$

It therefore follows from (2.8) that

$$\sigma_2(q) \ge \{C_0 + o(1)\} \prod_{p<X^\delta} (1 - g_q(p)/p).$$

However, since q is odd we have

$$\prod_{p<X^\delta}(1-g_q(p)/p) \sim 2\prod_{p|q}(1-g(p)/p)^{-1}\prod_{p<X^\delta}(1-g(p)/p),$$

on noting that any prime factor p of q for which $p \geq X^\delta$ can have only a negligible effect. It follows that

$$\begin{aligned} f(q)\sum_{A|R,\,(A,q)=1}\lambda_{N(A)}\frac{\rho(A)}{N(A)} & \\ &= f(q)\sigma_2(q) \\ &\geq 2\{C_0+o(1)\}f(q)\prod_{p|q}(1-g(p)/p)^{-1}\prod_{p<X^\delta}(1-g(p)/p) \\ &= 2\{C_0+o(1)\}h(q)\prod_{p<X^\delta}(1-g(p)/p). \end{aligned}$$

Lemma 6 is now a consequence of this estimate along with equations (6.1) and (6.3).

7 Proof of Lemma 7

This section will be devoted to the proof of Lemma 7. The necessary ideas may be traced back to work of Greaves [3]. We begin with the following result.

Lemma 10 *Let*

$$\begin{aligned} S(R) &= S(R;A,B,U) \\ &= \#\{a,b:\ A<a\leq A+U,\ B<b\leq B+U,\ R|a-b\sqrt[3]{2}\}. \end{aligned}$$

Then

$$\sum_{N(R)\leq Q,\,\rho(R)=1}|S(R)-\frac{U^2}{N(R)}| \ll (U+Q)Q^\varepsilon, \tag{7.1}$$

for any $\varepsilon>0$.

To establish Lemma 10 we begin by splitting the vectors (a,b) into congruence classes modulo $N(R)$, whence

$$\begin{aligned} S(R) &= \sum_{\substack{u,v\ (\mathrm{mod}\ N(R))\\ R|u-v\sqrt[3]{2}}}\#\{a,b:\ a\equiv u,\ b\equiv v\ (\mathrm{mod}\ N(R))\} \\ &= N(R)^{-2}\sum_{\substack{u,v\ (\mathrm{mod}\ N(R))\\ R|u-v\sqrt[3]{2}}}\sum_{c,d\ (\mathrm{mod}\ N(R))}\sum_{a,b}e_{N(R)}(c(u-a)+d(v-b)) \\ &= N(R)^{-2}\sum_{c,d\ (\mathrm{mod}\ N(R))}S_0(R,c,d)\sum_{a,b}e_{N(R)}(-ca-db) \end{aligned}$$

where

$$S_0(R,c,d) = \sum_{\substack{u,v \pmod{N(R)} \\ R|u-v\sqrt[3]{2}}} e_{N(R)}(cu+dv).$$

To evaluate the sum $S_0(R,c,d)$ we observe that there is a rational integer k, say, such that $k \equiv \sqrt[3]{2} \pmod{R}$, since $\rho(R)=1$. The condition $R|u-v\sqrt[3]{2}$ is therefore equivalent to $R|u-vk$. However, if $R|u-vk$ we must have $N(R)|u-vk$, again using the fact that $\rho(R)=1$. We therefore see that

$$S_0(R,c,d) = \sum_{v \pmod{N(R)}} e_{N(R)}(cvk+dv),$$

whence $S_0(R,c,d) = N(R)$ for $N(R)|ck+d$, and $S_0(R,c,d)=0$ otherwise. Reversing the argument above one finds that the condition $N(R)|ck+d$ is equivalent to $R|d+c\sqrt[3]{2}$.

Since $S_0(R,0,0)=N(R)$, we obtain

$$\begin{aligned} S(R) &= \frac{U^2+O(U)}{N(R)} \\ &+ O\Big(N(R)^{-1} \sum_{\substack{|c|,|d|\le N(R)/2 \\ (c,d)\neq(0,0),\, R|d+c\sqrt[3]{2}}} \min\{U, \frac{N(R)}{|c|}\} \min\{U, \frac{N(R)}{|d|}\}\Big). \end{aligned} \tag{7.2}$$

The total contribution from the first error term on the right is

$$\ll U \sum_{N(R)\le Q} N(R)^{-1} \ll U(\log Q),$$

which is satisfactory for Lemma 10.

We proceed to estimate the contribution to (7.1) arising from terms in (7.2) for which c,d are both non-zero. This is

$$\begin{aligned} &\ll Q \sum_{0<|c|,|d|\le Q} |cd|^{-1} \#\{N(R)\le Q:\ R|d+c\sqrt[3]{2}\} \\ &\ll Q \sum_{0<|c|,|d|\le Q} |cd|^{-1} Q^{\varepsilon} \\ &\ll Q^{1+2\varepsilon}, \end{aligned}$$

which is satisfactory for Lemma 10.

We turn now to the terms of (7.2) in which c, say, is zero. By the same argument as before we find that the corresponding contribution to (7.1) is

$$\begin{aligned} &\ll U \sum_{0<|d|\le Q} |d|^{-1} \#\{N(R)\le Q:\ R|d\} \\ &\ll U \sum_{0<|d|\le Q} |d|^{-1}|d|^{\varepsilon} \\ &\ll UQ^{\varepsilon}. \end{aligned}$$

Again this is satisfactory for Lemma 10. An entirely analogous argument applies for terms with $d = 0$, thereby completing the proof of the lemma.

Our next task is to derive a version of Lemma 10 in which one only counts terms with $(a, b) = 1$.

Lemma 11 *Let*

$$T(R) = \#\{a, b : A < a \le A + M,\ B < b \le B + M,\ (a, b) = 1,\ R|a - b\sqrt[3]{2}\},$$

and let

$$\gamma(R) = \prod_{p|N(R)} (1 + \frac{1}{p})^{-1}.$$

Then

$$\sum_{N(R)\le Q} |T(R) - \frac{6}{\pi^2}\frac{M^2}{N(R)}\gamma(R)\rho(R)| \ll (NQ^{1/2} + N^{3/2})N^{\varepsilon},$$

for any $Q \le N^2$ and any $\varepsilon > 0$.

For the proof we begin by noting that $T(R)$ vanishes unless $\rho(R) = 1$, as we henceforth assume. We next observe that

$$T(R) = \sum_{d=1}^{\infty} \mu(d) T_d(R),$$

with

$$T_d(R) = \#\{a, b : A < a \le A + M,\ B < b \le B + M,\ d|a,\ d|b,\ R|a - b\sqrt[3]{2}\}.$$

Writing $a = da', b = db'$ we find that

$$T(R) = \sum_{d=1}^{\infty} \mu(d) S(R'; A', B', M'), \tag{7.3}$$

where $A' = A/d, B' = B/d, M' = M/d$ and $R' = R(R, d)^{-1}$. Moreover, if $\rho(R) = 1$ we have

$$\begin{aligned} \sum_{d=1}^{\infty} \mu(d)\frac{M^2}{d^2} N(R/(R, d))^{-1} &= \frac{M^2}{N(R)} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} N((R, d)) \qquad (7.4)\\ &= \frac{M^2}{N(R)} \prod_{p\nmid N(R)} (1 - \frac{1}{p^2}) \prod_{p|N(R)} (1 - \frac{1}{p})\\ &= \frac{6M^2}{\pi^2 N(R)} \prod_{p|N(R)} (1 + \frac{1}{p})^{-1}, \end{aligned}$$

which produces the leading terms in Lemma 11.

We shall split the sums (7.3) and (7.4) at $d = \Delta$, where $1 \le \Delta \le N$ will be specified below. Terms in (7.4) for which $d > \Delta$ contribute a total

$$\ll \sum_{\substack{N(R)\le Q\\ \rho(R)=1}} \frac{M^2}{N(R)} \sum_{d>\Delta} d^{-2} N((R, d))$$

in Lemma 11. We put $(R,d)=S$ and $R=ST$. Thus $N(S)|d$, since $\rho(R)=1$, and on setting $d=N(S)e$, the above becomes

$$\begin{aligned}
&\ll M^2 \sum_{N(ST)\le Q} N(S)^{-2}N(T)^{-1} \sum_{e>\Delta/N(S)} e^{-2} \\
&\ll M^2 \sum_{N(S),N(T)\le Q} N(S)^{-2}N(T)^{-1}\min\{1,N(S)/\Delta\} \\
&\ll M^2\Delta^{-1}(\log N)^2. \qquad (7.5)
\end{aligned}$$

Similarly, the contribution from the terms of (7.3) in which $d>\Delta$ is

$$\begin{aligned}
&\ll \sum_{N(R)\le Q}\sum_{d>\Delta} S(\frac{R}{(R,d)};\frac{A}{d},\frac{B}{d},\frac{M}{d}) \\
&\ll \sum_{d>\Delta}\sum_{N(S)|d}\sum_{N(T)\le Q/N(S)} S(T;\frac{A}{d},\frac{B}{d},\frac{M}{d}) \\
&\ll \sum_{d>\Delta} d^{\varepsilon}\sum_{a',b'}\tau(a'-b'\sqrt[3]{2}) \\
&\ll N^{\varepsilon}\sum_{\Delta<d\ll N}(\frac{N}{d})^2N^{\varepsilon} \\
&\ll N^{2+2\varepsilon}\Delta^{-1}. \qquad (7.6)
\end{aligned}$$

Here we have used (2.21) and observed that, since $A,B,M\ll N$, the number of integer pairs a',b' with

$$\frac{A}{d}<a'\le\frac{A+M}{d},\quad \frac{B}{d}<b'\le\frac{B+M}{d}$$

is zero unless $d\ll N$, in which case it is $O(N^2d^{-2})$.

If we now write $S=(R,d)$ and $R=ST$ once more, it follows via Lemma 10 that the overall contribution from terms of (7.3) and (7.4) with $d\le\Delta$ is

$$\begin{aligned}
&\ll \sum_{\substack{N(R)\le Q\\ \rho(R)=1}}\sum_{d\le\Delta}|S(\frac{R}{(R,d)};\frac{A}{d},\frac{B}{d},\frac{M}{d})-\frac{(M/d)^2}{N(R/(R,d))}| \\
&\ll \sum_{d\le\Delta}\sum_{N(S)|d}\sum_{\substack{N(T)\le Q/N(S)\\ \rho(T)=1}}|S(T;\frac{A}{d},\frac{B}{d},\frac{M}{d})-\frac{(M/d)^2}{N(T)}| \\
&\ll \sum_{d\le\Delta}\sum_{N(S)|d}(\frac{M}{d}+\frac{Q}{N(S)})N^{\varepsilon} \\
&\ll \Delta(M+Q)N^{2\varepsilon}.
\end{aligned}$$

On comparing this with (7.5) and (7.6) we find that the sum in Lemma 11 is

$$\ll\{N^2\Delta^{-1}+\Delta(M+Q)\}N^{2\varepsilon}.$$

We shall choose $\Delta = \min(N^{1/2}, NQ^{-1/2})$, which does indeed satisfy the condition $1 \le \Delta \le N$, and yields a bound

$$\ll (NQ^{1/2} + N^{3/2})N^{2\varepsilon},$$

thus completing the proof of Lemma 11.

We may now deduce Lemma 7. In view of the definition of $h(q)$ we may include an extra summation condition $(a,b) = 1$ in (2.20). Moreover, we have

$$h(q) = \sum_{d|q} l(d),$$

where $l(d)$ is the multiplicative function defined by (2.18) and (2.19). It follows that

$$C(q_1q_2) = \sum_d l(d)C'([q_1q_2, d]),$$

with

$$C'(m) = \#\{a, b:\ A < a \le A + M,\ B < b \le B + M,\ (a,b) = 1,\ m|q\},$$

and hence that

$$\begin{aligned}\sum_{q_1,q_2} |C(q_1q_2) - C_1M^2\frac{\nu(q_1)\nu(q_2)}{q_1q_2}| \\ = \sum_{q_1,q_2} |\sum_{d=1}^{\infty} l(d)C'([q_1q_2,d]) - C_1M^2\frac{\nu(q_1)\nu(q_2)}{q_1q_2}|. \end{aligned} \tag{7.7}$$

We begin by considering the contribution to (7.7) arising from terms with $d \ge D$, say. This is at most

$$\sum_{q_1,q_2}\sum_{d\ge D} |l(d)C'([q_1q_2,d])|. \tag{7.8}$$

If $l(d) \ne 0$ we may write $d = ef^2$ with e, f coprime and square-free. Moreover we then have $l(d) \ll d^{\varepsilon}e^{-1}$, for any $\varepsilon > 0$. We also note that if f is coprime to q_1q_2 then

$$[q_1q_2, d] \ge q_1q_2f^2 \ge N^{11/7}f^2.$$

We may therefore assume that $f \ll N^{5/7}$ for such f, since $C'(m)$ clearly vanishes for $m \gg N^3$. When $(f, q_1q_2) = 1$ and $e \ge D^{1/2}$, say, the contribution to (7.8) is then

$$\begin{aligned} &\ll N^{\varepsilon}D^{-1/2}\sum_{a,b} \#\{(q_1,q_2,e,f):\ q_1,q_2,e,f|a^3 - 2b^3\} \\ &\ll N^{\varepsilon}D^{-1/2}\sum_{a,b} N^{\varepsilon} \\ &\ll M^2N^{2\varepsilon}D^{-1/2}, \end{aligned} \tag{7.9}$$

while the contribution from terms with $(f, q_1q_2) = 1$ and $e < D^{1/2}$ is

$$\begin{aligned} &\ll N^{\varepsilon}\sum_{D^{1/4}<f\ll N^{5/7}}\ \sum_{a,b:\, f^2|a^3-2b^3} \#\{(q_1,q_2,e):\ q_1,q_2,e|a^3 - 2b^3\} \\ &\ll N^{\varepsilon}\sum_{D^{1/4}<f\ll N^{5/7}}\ \sum_{a,b:\, f^2|a^3-2b^3} N^{\varepsilon}. \end{aligned} \tag{7.10}$$

Here we observe that if $f^2|a^3-2b^3$ then f and b must be coprime, since a and b are. Thus $a^3 \equiv 2b^3 \pmod{f^2}$ determines $O(f^\varepsilon)$ values of a modulo f^2 for each choice of b. It follows that

$$\#\{a,b:\ f^2|a^3-2b^3\} \ll N^\varepsilon M(1+Mf^{-2}), \tag{7.11}$$

whence (7.10) is

$$\ll N^{3\varepsilon} \sum_{D^{1/4}<f\ll N^{5/7}} (M+M^2f^{-2}) \ll N^{3\varepsilon}(MN^{5/7}+M^2D^{-1/4}). \tag{7.12}$$

It remains to consider the contribution to (7.8) from terms for which q_1, say, divides f. If we write $f=q_1g$, then this is

$$\begin{aligned} &\ll \sum_{q_1} \sum_{a,b:\, q_1^2|a^3-2b^3} \#\{(q_2,e,g):\ q_2,e,g|a^3-2b^3\} \\ &\ll \sum_{q_1} \sum_{a,b:\, q_1^2|a^3-2b^3} N^\varepsilon \\ &\ll N^{2\varepsilon}\sum_{q_1}(M+M^2q_1^{-2}) \\ &\ll N^{2\varepsilon}(MN^{5/7+\delta}+M^2N^{-5/7}), \end{aligned} \tag{7.13}$$

on applying (7.11) with $f=q_1$. Similarly, terms with $q_2|f$ contribute

$$\ll N^{2\varepsilon}(MN^{6/7+\delta}+M^2N^{-6/7}). \tag{7.14}$$

In view of (2.6) we see that the bounds (7.9), (7.12), (7.13) and (7.14) will be satisfactory for Lemma 7, providing that we choose $D=N^{5\delta}$, as we now do. To be specific we will have

$$\begin{aligned} &\sum_{q_1,q_2} |C(q_1q_2) - C_1M^2\frac{\nu(q_1)\nu(q_2)}{q_1q_2}| \\ &\quad = \sum_{q_1,q_2} |\sum_{d<D} l(d)C'([q_1q_2,d]) - C_1M^2\frac{\nu(q_1)\nu(q_2)}{q_1q_2}| + O(M^2N^{-\delta}), \end{aligned}$$

by (7.7).

We now examine the representation

$$C_1 = \frac{6}{\pi^2}\sum_{d=1}^{\infty} l(d)\frac{\nu(d)}{d}.$$

We have

$$\frac{\nu(q_1q_2)}{q_1q_2}\sum_{d<D} l(d)\frac{\nu(d)}{d} = \sum_{d<D} l(d)\frac{\nu([q_1q_2,d])}{[q_1q_2,d]},$$

since d is coprime to q_1q_2 for $d < N^{5\delta}$. Moreover, if we take $d = ef^2$, with e, f coprime and square-free, then

$$\begin{aligned}\sum_{d\geq D} l(d)\frac{\nu(d)}{d} &\ll \sum_{ef^2\geq D} (ef)^{-2+\varepsilon} \\ &\ll \sum_{ef\geq D^{1/2}} (ef)^{-2+\varepsilon} \\ &\ll \sum_{n\geq D^{1/2}} n^{-2+2\varepsilon} \\ &\ll D^{-1/2+\varepsilon} \\ &\ll N^{-\delta}.\end{aligned}$$

Since

$$\sum_{q_1,q_2} \frac{\nu(q_1)\nu(q_2)}{q_1q_2} \ll 1$$

we may conclude that

$$\sum_{q_1,q_2} |C_1M^2\frac{\nu(q_1)\nu(q_2)}{q_1q_2} - \frac{6}{\pi^2}M^2\sum_{d<D} l(d)\frac{\nu([q_1q_2,d])}{[q_1q_2,d]}| \ll M^2N^{-\delta},$$

whence

$$\begin{aligned}&\sum_{q_1,q_2} |C(q_1q_2) - C_1M^2\frac{\nu(q_1)\nu(q_2)}{q_1q_2}| \\ &\quad\ll M^2N^{-\delta} + \sum_{q_1,q_2}\sum_{d<D} |l(d)\{C'([q_1q_2,d]) - \frac{6}{\pi^2}\frac{M^2}{[q_1q_2,d]}\nu([q_1q_2,d])\}| \\ &\quad\ll M^2N^{-\delta} + N^{\varepsilon}\sum_{q_1,q_2,d} |C'([q_1q_2,d]) - \frac{6}{\pi^2}\frac{M^2}{[q_1q_2,d]}\nu([q_1q_2,d])| \\ &\quad\ll M^2N^{-\delta} + N^{2\varepsilon}\sum_{r\ll N^{11/7+7\delta}} |C'(r) - \frac{6}{\pi^2}\frac{M^2}{r}\nu(r)|. \qquad (7.15)\end{aligned}$$

It is an easy exercise to verify that, if $(a,b) = 1$, then there is a 1-1 correspondence between divisors r of $a^3 - 2b^3$ and ideal divisors R of $a - b\sqrt[3]{2}$, given by $r \to (r, a - b\sqrt[3]{2}) = R$ and $R \to N(R) = r$. Moreover one readily checks that

$$\nu(r) = \sum_{N(R)=r} \gamma(R)\rho(R).$$

Thus (7.15) is

$$\begin{aligned}&\ll M^2N^{-\delta} + N^{2\varepsilon}\sum_{N(R)\ll N^{11/7+7\delta}} |T(R) - \frac{6}{\pi^2}\frac{M^2}{N(R)}\gamma(R)\rho(R)| \\ &\ll M^2N^{-\delta} + (N.N^{(11/7+7\delta)/2} + N^{3/2})N^{\varepsilon} \\ &\ll M^2N^{-\delta} + N^{25/14+7\delta/2+\varepsilon},\end{aligned}$$

by Lemma 11. This clearly suffices for Lemma 7, since

$$N^{25/14+7\delta/2+\varepsilon} \ll M^2N^{-\delta},$$

for ε sufficiently small.

8 The Lower Bound for S_0

In this section we shall prove Lemmas 8 and 9. To handle the sum

$$\sum_{a,b:\, q\in\mathcal{Q}} I(a,b)h(q),$$

where

$$I(a,b)=\int_{(a,b,t)\in\mathcal{R}} N(a,b,t)^{-1}dt$$

we shall divide the available range for the variables a,b and t into disjoint cubes

$$\mathcal{B}=(A,A+M]\times(B,B+M]\times(C,C+M]\subseteq\mathbb{R}^3.$$

We shall call such a cube 'good' if it falls entirely inside the region $\mathcal{R}_0$ given by the constraints

$$M^3X^{\delta/2}=X^{1+3\delta/2}<N(\mathbf{x})<N^3=X^{1+2\delta}, \tag{8.1}$$

$$1<\frac{x_1+x_2\sqrt[3]{2}+x_3\sqrt[3]{4}}{N(\mathbf{x})^{1/3}}<\varepsilon_0, \tag{8.2}$$

and

$$x_1^3-2x_2^3>M^3.$$

Plainly we then have

$$\sum_{a,b:\, q\in\mathcal{Q}} I(a,b)h(q)\geq\sum_{\mathcal{B}}\sum_{a,b}h(q)\int_{(a,b,t)\in\mathcal{B}}N(a,b,t)^{-1}dt, \tag{8.3}$$

where only good cubes $\mathcal{B}$ are counted, and the sum over a,b is restricted by the condition (2.17).

In view of (4.1), if $N(\mathbf{x})$ attains its maximum on $\mathcal{B}$ at $\mathbf{x}_0$, we have

$$N(\mathbf{x})=N(\mathbf{x}_0)+O(MN(\mathbf{x}_0)^{2/3}) \tag{8.4}$$

for any $\mathbf{x}\in\mathcal{B}$. Since $N(\mathbf{x}_0)\gg M^3X^{\delta/2}$ it follows that $N(\mathbf{x})\gg N(\mathbf{x}_0)$ for all $\mathbf{x}\in\mathcal{B}$, whence

$$N(A,B,C)\ll N(\mathbf{x})\ll N(A,B,C)\quad(\mathbf{x}\in\mathcal{B}).$$

We may then apply (5.2) to show that

$$N(\mathbf{x})^{-1}=N(A,B,C)^{-1}+O(MN(A,B,C)^{-4/3}), \tag{8.5}$$

whence

$$\begin{aligned}\int_{(a,b,t)\in\mathcal{B}}N(a,b,t)^{-1}dt &= \frac{M}{N(A,B,C)}+O(M^2N(A,B,C)^{-4/3})\\ &= \{1+o(1)\}\frac{M}{N(A,B,C)},\end{aligned}$$

by (8.1). We may therefore deduce from (8.3) that

$$\sum_{a,b:\, q\in\mathcal{Q}} I(a,b)h(q)\geq\{1+o(1)\}\sum_{\mathcal{B}}\frac{M}{N(A,B,C)}\sum_{a,b}h(q), \tag{8.6}$$

subject to the same restrictions on $\mathcal{B}$ and a, b as before.

We now observe that if $q \ll N^3$ has m distinct prime divisors in the range $N^{5/7} < p \leq N^{5/7+\delta}$, and n in the range $N^{6/7} < p \leq N^{6/7+\delta}$, then $mn \leq 3$. It follows that q can be counted with multiplicity at most 3 in the sum

$$\sum_{q_1, q_2} C(q_1 q_2).$$

We therefore see, via Lemma 7, that for any given good cube $\mathcal{B}$, we have

$$\begin{aligned} \sum_{a,b} h(q) &\geq \frac{1}{3} \sum_{q_1, q_2} C(q_1 q_2) \\ &= \frac{1}{3} C_1 M^2 \sum_{q_1, q_2} \frac{\nu(q_1)\nu(q_2)}{q_1 q_2} + O(M^2 N^{-\delta}). \end{aligned}$$

Moreover

$$\sum_{p \leq x} \nu(p)/p = \log\log x + C + o(1),$$

for a suitable constant C, by the Prime Ideal Theorem, whence

$$\sum_{q_1, q_2} \frac{\nu(q_1)\nu(q_2)}{q_1 q_2} = L(\delta) + o(1),$$

and hence

$$\sum_{a,b} h(q) \geq \frac{1}{3} C_1 M^2 \{1 + o(1)\} L(\delta).$$

We may combine this with (8.6) to deduce that

$$\sum_{a,b:\, q \in \mathcal{Q}} I(a,b) h(q) \geq \frac{1}{3} C_1 \{1 + o(1)\} L(\delta) \sum_{\mathcal{B}} \frac{M^3}{N(A,B,C)}.$$

A second application of (8.4) now shows that

$$\frac{M^3}{N(A,B,C)} = \{1 + o(1)\} \int_{\mathcal{B}} \frac{dx\, dy\, dz}{N(x,y,z)},$$

whence

$$\sum_{\mathcal{B}} \frac{M^3}{N(A,B,C)} = \{1 + o(1)\} \int_{\mathcal{R}_1} \frac{dx\, dy\, dz}{N(x,y,z)},$$

where $\mathcal{R}_1$ is the part of the region $\mathcal{R}_0$ made up of points in good cubes. It follows that

$$\sum_{a,b:\, q \in \mathcal{Q}} I(a,b) h(q) \geq \frac{1}{3} C_1 \{1 + o(1)\} L(\delta) I_1, \tag{8.7}$$

where

$$I_1 = \int_{\mathcal{R}_1} \frac{dx\, dy\, dz}{N(x,y,z)}.$$

We now aim to compare I_1 with the integral

$$I_2 = \int_{\mathcal{R}_2} \frac{dx\, dy\, dz}{N(x,y,z)},$$

where $\mathcal{R}_2$ is defined by the constraints

$$M^3 X^{\delta/2} = X^{1+3\delta/2} < N(\mathbf{x}) < N^3 = X^{1+2\delta},$$

$$1 < \frac{x_1 + x_2\sqrt[3]{2} + x_3\sqrt[3]{4}}{N(\mathbf{x})^{1/3}} < \varepsilon_0,$$

and

$$x_1^3 - 2x_2^3 > 0. \tag{8.8}$$

In order to do this we make a change of variables

$$x = \frac{1}{3}(w + 2r\cos\theta), \quad y = \frac{1}{3\sqrt[3]{2}}(w + 2r\cos(\theta + 4\pi/3)),$$

$$z = \frac{1}{3\sqrt[3]{4}}(w + 2r\cos(\theta + 2\pi/3)),$$

where $r > 0$ and $0 \le \theta < 2\pi$, so that

$$x + y\sqrt[3]{2} + z\sqrt[3]{4} = w, \quad x + y\omega\sqrt[3]{2} + z\omega^2\sqrt[3]{4} = re^{i\theta} \quad (\omega = e^{2\pi i/3}).$$

The Jacobian of this transformation is $r/3\sqrt{3}$, whence

$$\int_{x,y,z} \frac{dx\,dy\,dz}{N(x,y,z)} = \frac{1}{3\sqrt{3}} \int_{w,r,\theta} \frac{dw\,dr\,d\theta}{wr}.$$

We also note that

$$x^3 - 2y^3 = \frac{2}{3\sqrt{3}} r|w - re^{i(\theta+2\pi/3)}|^2 \sin(\theta + 2\pi/3). \tag{8.9}$$

The condition (8.8) is therefore equivalent to $\sin(\theta + 2\pi/3) > 0$. It follows that

$$I_2 = \frac{1}{3\sqrt{3}} \int_{w,r,\theta} \frac{dw\,dr\,d\theta}{wr},$$

subject to

$$X^{1+3\delta/2} < wr^2 < X^{1+2\delta},$$

$$1 < (\frac{w}{r})^{2/3} < \varepsilon_0,$$

and

$$\sin(\theta + 2\pi/3) > 0.$$

This produces

$$I_2 = \frac{\pi}{3\sqrt{3}} \int_{w,r} \frac{dw\,dr}{wr}.$$

A further substitution $w = \mu^{1/3}\nu$, $r = \mu^{1/3}\nu^{-1/2}$, for which the Jacobian is $\frac{1}{2}\mu^{-1/3}\nu^{-1/2}$, yields

$$I_2 = \frac{\pi}{6\sqrt{3}} \int_{\mu,\nu} \frac{d\mu\,d\nu}{\mu\nu}.$$

Since the region of integration is now merely

$$X^{1+3\delta/2} < \mu < X^{1+2\delta}, \quad 1 < \nu < \varepsilon_0,$$

we deduce that

$$I_2 = \frac{\pi}{6\sqrt{3}} \frac{\delta}{2} (\log X)(\log \varepsilon_0).$$

We must now estimate $I_2 - I_1$. Any point $\mathbf{x} \in \mathcal{R}_0 \setminus \mathcal{R}_1$ must lie a distance $O(M)$ from a boundary point $\mathbf{x}'$, say of the region $\mathcal{R}_0$. The argument leading to (8.4) then shows that

$$N(\mathbf{x}) = N(\mathbf{x}') + O(MN(\mathbf{x}')^{2/3}).$$

Thus if $N(\mathbf{x}') = X^{1+2\delta}$ then

$$N(\mathbf{x}) = X^{1+2\delta} + O(X^{1+5\delta/3}), \tag{8.10}$$

and if $N(\mathbf{x}') = X^{1+3\delta/2}$ then

$$N(\mathbf{x}) = X^{1+3\delta/2} + O(X^{1+4\delta/3}). \tag{8.11}$$

Moreover, (5.2) yields

$$\frac{\partial}{\partial x_i} \frac{x_1 + x_2 \sqrt[3]{2} + x_3 \sqrt[3]{4}}{N(\mathbf{x})^{1/3}} \ll N(\mathbf{x})^{-1/3},$$

so that

$$\begin{aligned} \frac{x_1 + x_2 \sqrt[3]{2} + x_3 \sqrt[3]{4}}{N(\mathbf{x})^{1/3}} &= \frac{x_1' + x_2' \sqrt[3]{2} + x_3' \sqrt[3]{4}}{N(\mathbf{x}')^{1/3}} + O(M(X^{1+3\delta/2})^{-1/3}) \\ &= \frac{x_1' + x_2' \sqrt[3]{2} + x_3' \sqrt[3]{4}}{N(\mathbf{x}')^{1/3}} + O(X^{-\delta/6}). \end{aligned}$$

Thus if

$$\frac{x_1' + x_2' \sqrt[3]{2} + x_3' \sqrt[3]{4}}{N(\mathbf{x}')^{1/3}} = 1 \quad \text{or} \quad \varepsilon_0,$$

then

$$\frac{x_1 + x_2 \sqrt[3]{2} + x_3 \sqrt[3]{4}}{N(\mathbf{x})^{1/3}} = 1 + O(X^{-\delta/6}) \quad \text{or} \quad \varepsilon_0 + O(X^{-\delta/6}), \tag{8.12}$$

respectively. Finally,

$$x_1'^3 - 2x_2'^3 = x_1^3 - 2x_2^3 + O(MN(\mathbf{x})^{2/3})$$

so that

$$x_1'^3 - 2x_2'^3 = M^3$$

implies

$$x_1^3 - 2x_2^3 \ll MN(\mathbf{x})^{2/3}. \tag{8.13}$$

To put this final condition into a more suitable form we note that $r \ll |w| \ll r$, by (8.2), whence (8.9) yields

$$|x_1^3 - 2x_2^3| \gg N(\mathbf{x}) |\sin(\theta + 2\pi/3)|.$$

Thus (8.13) produces

$$\sin(\theta + 2\pi/3) \ll MN(\mathbf{x})^{-1/3} \ll X^{-\delta/6}. \tag{8.14}$$

We also observe that if $\mathbf{x} \in \mathcal{R}_2 \setminus \mathcal{R}_0$ then (8.13) holds, so that we again have (8.14).

We can now estimate $I_2 - I_1$ by using exactly the same changes of variables as were employed in our treatment of I_2. If (8.10) holds then the range for μ becomes $\mu = X^{1+2\delta} + O(X^{1+5\delta/3})$, and the overall contribution to $I_2 - I_1$ is $O(X^{-\delta/3})$. Similarly when (8.11) holds we have $\mu = X^{1+3\delta/2} + O(X^{1+4\delta/3})$, which contributes $O(X^{-\delta/6})$. For those values of $\mathbf{x}$ for which one or other of the constraints (8.12) hold the variable ν is restricted to an interval of length $O(X^{-\delta/6})$, so that there is a contribution to $I_2 - I_1$ of size $O(X^{-\delta/6})$. Finally when we have (8.14), the variable θ is restricted to lie in an interval of length $O(X^{-\delta/6})$, with a corresponding contribution to $I_2 - I_1$. We therefore conclude that

$$I_2 - I_1 \ll X^{-\delta/6},$$

so that

$$I_1 \sim \frac{\pi}{6\sqrt{3}} \frac{\delta}{2} (\log X)(\log \varepsilon_0).$$

We now deduce from (8.7) that

$$\sum_{a,b:\, q \in \mathcal{Q}} I(a,b)h(q) \geq \frac{1}{3} C_1 \{1 + o(1)\} L(\delta) \frac{\pi}{6\sqrt{3}} \frac{\delta}{2} (\log X)(\log \varepsilon_0),$$

so that Lemma 8 follows from Lemma 6.

We move now to the treatment of Lemma 9. We begin by observing that

$$\sum_{x < p \leq y} \log(1 - \frac{g(p)}{p^\sigma}) - \log(1 - \frac{1}{p^\sigma}) = \sum_{x < p \leq y} \frac{1 - g(p)}{p^\sigma} + O(x^{-1}),$$

uniformly for $\sigma \geq 1$. Moreover, the Prime Ideal Theorem and the Prime Number Theorem show that

$$\sum_{p \leq z} (1 - g(p)) \ll z(\log z)^{-2},$$

since prime ideals of degree 2 or 3 make a negligible contribution. It follows by partial summation that

$$\sum_{x < p \leq y} \frac{1 - g(p)}{p^\sigma} \ll (\log x)^{-1},$$

uniformly for $\sigma \geq 1$, whence

$$\sum_{x < p \leq y} \log(1 - \frac{g(p)}{p^\sigma}) - \log(1 - \frac{1}{p^\sigma}) \ll (\log x)^{-1}.$$

We may therefore deduce that

$$\prod_{p \leq x} \frac{1 - g(p)/p^\sigma}{1 - 1/p^\sigma} = \{1 + O(\frac{1}{\log x})\} \prod_p \frac{1 - g(p)/p^\sigma}{1 - 1/p^\sigma},$$

the final product being over all primes. However

$$\prod_p \frac{1 - g(p)/p^\sigma}{1 - 1/p^\sigma} = F(\sigma)\zeta(\sigma)\zeta_{\mathbb{Q}(\sqrt[3]{2})}(\sigma)^{-1},$$

where

$$F(\sigma) = \prod_p \{(1 - g(p)/p^\sigma) \prod_{N(P)=p} (1 - 1/N(P)^\sigma)^{-1}\}.$$

This last product is absolutely and uniformly convergent for $\sigma \geq 1$, so that $F(\sigma) \to F(1)$ as σ tends down to 1. On the other hand

$$\zeta(\sigma)\zeta_{\mathbb{Q}(\sqrt[3]{2})}(\sigma)^{-1} \to \frac{1}{\mathrm{Res}(\zeta_{\mathbb{Q}(\sqrt[3]{2})}(s);\ s=1)} = \frac{\sqrt{27}}{\pi \log \varepsilon_0},$$

as σ tends down to 1. We conclude that

$$\prod_{p \leq x} \frac{1 - g(p)/p}{1 - 1/p} = \{1 + O(\frac{1}{\log x})\}F(1)\frac{\sqrt{27}}{\pi \log \varepsilon_0}.$$

To complete the proof of Lemma 9 we have merely to note that

$$\prod_{p \leq x} (1 - 1/p) \sim \frac{e^{-\gamma}}{\log x},$$

by Mertens' Theorem.

9 Proof of Theorem 2

We may observe at the outset that Theorem 2 is trivially true if the polynomial $g(X)$ is not coprime to q, since the sum will be empty. We shall therefore suppose henceforth that $(g(X), q) = 1$.

We shall prove Theorem 2 by induction on k, and so we begin by examining the case $k = 0$. Here we find in the usual way that if

$$S = \sum_{A < n \leq A+B} e_q(wf(n)\overline{g(n)}^{(q)}),$$

then

$$S = \frac{1}{q} \sum_{m \pmod q} S(q, m, 1) \sum_{A < n \leq a+B} e_q(-mn), \tag{9.1}$$

where

$$S(q, m, a) = \sum_{h \pmod q} e_q(a\{wf(h)\overline{g(h)}^{(q)} + mh\}).$$

The above sum has a multiplicative property,

$$S(uv, m, a) = S(u, m, a\overline{v}^{(u)})S(v, m, a\overline{u}^{(v)}),$$

for $(u, v) = 1$. Moreover, if p is prime, and $p \nmid a$ but $p|w$, then

$$S(p, m, a) = \begin{cases} 0, & p \nmid m, \\ p, & p|m. \end{cases}$$

It therefore follows that $S(q, m, 1)$ vanishes unless $\Delta|m$. In the latter case Weil's estimate shows that

$$|S(p, m, a)| \leq 2D\sqrt{p},$$

for $p \nmid aw$, providing that $f(X)/g(X)$ does not reduce to a linear (or constant) polynomial modulo p. Under the latter assumption we therefore have

$$|S(p,m,a)| \le 2D(w,p)^{1/2}p^{1/2},$$

for $p \nmid a$, whether or not w is coprime to p. We now apply the hypotheses of Theorem 2, noting that $q = q_0$. This allows us to deduce that

$$|S(q,m,1)| \le d_{2D}(q)(\Delta q)^{1/2},$$

when $\Delta | m$. If we insert this bound into (9.1) we find that

$$\begin{aligned} S &\ll q^{-1} \sum_{m \pmod q,\, \Delta|m} d_{2D}(q)(\Delta q)^{1/2} \min\{B\,,\, ||m/q||^{-1}\} \\ &\ll q^{-1} d_{2D}(q)(\Delta q)^{1/2}\{B + \frac{q}{\Delta}\log q\} \\ &\ll d_{2D}(q)\{B(\Delta/q)^{1/2} + (q/\Delta)^{1/2}\}\log q \\ &\ll_\varepsilon q^\varepsilon\{B(\Delta/q)^{1/2} + (q/\Delta)^{1/2}\}, \end{aligned}$$

as required for the case $k = 0$ of Theorem 2.

To establish the general case of Theorem 2 by induction we shall assume it holds true when q has an expression $q = q_0'q_1' \dots q_{k-1}'$, and deduce that it holds for a representation $q = q_0q_1 \dots q_k$. For ease of notation we write

$$a(n) = \begin{cases} e_q(wf(n)\overline{g(n)}^{(q)}), & A < n \le A+B, \\ 0, & \text{otherwise.} \end{cases}$$

Then, if $H = [B/q_k] + 1$ we find that

$$\begin{aligned} HS &= \sum_{h=1}^{H}\sum_n a(n+hq_k) \\ &= \sum_n\sum_{h=1}^{H} a(n+hq_k) \\ &= \sum_{A-Hq_k < n \le A+B-q_k}\ \sum_{h=1}^{H} a(n+hq_k). \end{aligned}$$

Thus Cauchy's inequality yields

$$\begin{aligned} H^2|S|^2 &\le (Hq_k + B - q_k)\sum_n |\sum_{h=1}^{H} a(n+hq_k)|^2 \\ &= (Hq_k + B - q_k)\sum_{h_1=1}^{H}\sum_{h_2=1}^{H}\sum_n a(n+h_1q_k)\overline{a(n+h_2q_k)} \\ &= (Hq_k + B - q_k)\sum_{h_1=1}^{H}\sum_{h_2=1}^{H}\sum_n a(n+\{h_1-h_2\}q_k)\overline{a(n)} \\ &\le 2BH \sum_{-H<h<H} |\sum_n a(n+hq_k)\overline{a(n)}| \\ &\le 2B^2H + 4BH\sum_{h=1}^{H-1} |\sum_n a(n+hq_k)\overline{a(n)}|. \end{aligned} \tag{9.2}$$

We now examine the function $a(n+hq_k)\overline{a(n)}$. Suppose that the polynomials $f(X)$ and $g(X)$ satisfy the conditions of Theorem 2. Let $t = hq_k$, and set

$$u(X) = \{g(X)f(X+t) - f(X)g(X+t)\}/t, \quad v(X) = g(X)g(X+t).$$

Then

$$f(n+t)\overline{g(n+t)}^{(q)} - f(n)\overline{g(n)}^{(q)} = tu(n)\overline{v(n)}^{(q)},$$

for $(g(n)g(n+t), q) = 1$. We proceed to show that Theorem 2 may be applied to

$$\sum_n a(n+hq_k)\overline{a(n)} = \sum_{A<n\le A+B-hq_k} e_q(whq_k u(n)\overline{v(n)}^{(q)}), \tag{9.3}$$

when $q = q_0'q_1'\dots q_{k-1}'$, with $q_0' = q_0q_k$ and $q_i' = q_i$ for $1 \le i < k$.

In order to do this we must verify that $u(X)$ and $v(X)$ satisfy the conditions of Theorem 2, with k replaced by $k-1$ and D replaced by $2D$. We first observe that $\deg(u(X)), \deg(v(X)) \le 2D$, and that $p > 2^{k-1} \times 2D$ for every prime $p|q$. Moreover, suppose that $u(X) \equiv v(X)h(X) \pmod p$ for some polynomial $h(X)$ with $\deg(h(X)) \le k$. We first examine the case in which $p \nmid t$. Then, in the field modulo p we may write (by abuse of notation),

$$\begin{aligned}\{g(X)f(X+t) - f(X)g(X+t)\}/t &= u(X)\\ &= v(X)h(X)\\ &= g(X)g(X+t)h(X).\end{aligned}$$

Let $f(X)$ and $g(X)$ have highest common factor $d(X)$, in the field modulo p, and put $f(X) = d(X)F(X)$ and $g(X) = d(X)G(X)$ accordingly, so that

$$G(X)F(X+t) - F(X)G(X+t) = tG(X)G(X+t)h(X). \tag{9.4}$$

Then $G(X)|F(X)G(X+t)$, whence $G(X)|G(X+t)$. In a similar way we find that $G(X+t)|G(X)$. Since $G(X)$ and $G(X+t)$ have the same leading coefficient, they must be equal. Then, since $p \nmid t$, and $\deg(G(X)) \le D < p$, we must conclude that $G(X)$ is constant, and without loss of generality we take $G(X) = 1$. The relation (9.4) then reduces to $F(X+t) - F(X) = th(X)$. Since $\deg(F(X)) \le D < p$, and $p \nmid t$ we have

$$\deg(F(X+t) - F(X)) = \deg(F(X)) - 1.$$

It then follows that $F(X)$ is a polynomial of degree at most $k+1$, since $\deg(h(X)) \le k$. We therefore find that

$$f(X) \equiv d(X)F(X) \equiv d(X)G(X)F(X) \equiv g(X)F(X) \pmod p,$$

contradicting the assumptions of Theorem 2.

Now assume that $p|t$. We have

$$\begin{aligned}&g(X)f(X+T) - f(X)g(X+T)\\ &\qquad = T\{g(X)f'(X) - f(X)g'(X)\} + T^2k(X,T),\end{aligned}$$

for a suitable polynomial $k(X,T)$. It follows that

$$u(X) = g(X)f'(X) - f(X)g'(X),$$

in the field modulo p. As before we write $f(X) = d(X)F(X)$ and $g(X) = d(X)G(X)$, where $d(X)$ is the highest common factor of $f(X)$ and $g(X)$, modulo p. It follows that

$$u(X) \equiv d(X)^2\{G(X)F'(X) - F(X)G'(X)\} \pmod{p}$$

Thus if $u(X) \equiv v(X)h(X) \pmod{p}$, then

$$G(X)F'(X) - F(X)G'(X) = G(X)G(X+t)h(X) = G(X)^2h(X), \qquad (9.5)$$

in the field modulo p. Since $G(X)$ is coprime to $F(X)$ it then follows that $G(X)|G'(X)$. However $G'(X)$ has smaller degree than $G(X)$, so that this can occur only when $G'(X) = 0$. As before we note that $\deg(G(X)) \le D < p$, so that we may deduce that $G(X)$ is constant, and without loss of generality we take $G(X) = 1$. The relation (9.5) then reduces to $F'(X) = h(X)$. Since $\deg(F(X)) \le D < p$ we deduce that $\deg(F(X)) = 1 + \deg(h(X)) \le 1 + k$. This then contradicts the hypotheses of Theorem 2, since

$$f(X) \equiv d(X)F(X) \equiv d(X)G(X)F(X) \equiv g(X)F(X) \pmod{p}.$$

Having checked that the hypotheses of Theorem 2 are verified for our application, we may deduce that the sum (9.3) is

$$\ll_{k,D,\varepsilon} q^{\varepsilon}\{B(\frac{\Delta'}{q_0'})^{1/2^k} + B^{1-1/2^{k-1}}(\frac{q_0'}{\Delta'})^{1/2^k} + \sum_{j=1}^{k-1} B^{1-1/2^j} {q'}_{k-j}^{1/2^j}\},$$

with $\Delta' = (q_0', whq_k)$. In view of our choice of the q_i' we conclude that

$$\sum_n a(n+hq_k)\overline{a(n)}$$

$$\ll_{k,D,\varepsilon} \quad q^{\varepsilon}\{B(\frac{\Delta''}{q_0})^{1/2^k} + B^{1-1/2^{k-1}}(\frac{q_0}{\Delta''})^{1/2^k} + \sum_{j=1}^{k-1} B^{1-1/2^j} q_{k-j}^{1/2^j}\},$$

with

$$\Delta'' = (q_0, wh) \le (q_0, w)(q_0, h) = \Delta(q_0, h).$$

We insert this into the bound (9.2), noting that

$$\begin{aligned}
\sum_{h=1}^{H-1}(q_0,h)^{1/2^k} &\le \sum_{h=1}^{H-1}(q_0,h) \\
&\le \sum_{m|q_0} m \sum_{h<H,\, m|h} 1 \\
&\le \sum_{m|q_0} m\frac{H}{m} \\
&= d(q_0)H \\
&\ll_{\varepsilon} q^{\varepsilon}H.
\end{aligned}$$

It then follows that

$$|S|^2 \ll_{k,D,\varepsilon}$$

$$B^2H^{-1} + q^{2\varepsilon}B\{B(\frac{\Delta}{q_0})^{1/2^k} + B^{1-1/2^{k-1}}(\frac{q_0}{\Delta})^{1/2^k} + \sum_{j=1}^{k-1} B^{1-1/2^j} q_{k-j}^{1/2^j}\}.$$

In view of our choice $H = [B/q_k] + 1$ this leads to the bound

$$|S|^2 \ll_{k,D,\varepsilon} q^{2\varepsilon}\{B^2(\frac{\Delta}{q_0})^{1/2^k} + B^{2-1/2^{k-1}}(\frac{q_0}{\Delta})^{1/2^k} + \sum_{j=0}^{k-1} B^{2-1/2^j} q_{k-j}^{1/2^j}\}.$$

We therefore have

$$\begin{aligned} S \quad &\ll_{k,D,\varepsilon} \quad q^{\varepsilon}\{B(\frac{\Delta}{q_0})^{1/2^{k+1}} + B^{1-1/2^k}(\frac{q_0}{\Delta})^{1/2^{k+1}} + \sum_{j=0}^{k-1} B^{1-1/2^{j+1}} q_{k-j}^{1/2^{j+1}}\} \\ &= \quad q^{\varepsilon}\{B(\frac{\Delta}{q_0})^{1/2^{k+1}} + B^{1-1/2^k}(\frac{q_0}{\Delta})^{1/2^{k+1}} + \sum_{j=1}^{k} B^{1-1/2^j} q_{k+1-j}^{1/2^j}\}, \end{aligned}$$

as required for our induction step. This completes the proof of Theorem 2.

10 Comparison with the Method of Hooley

We shall begin by looking at Chebyshev's original method, as used by Hooley. We shall do this in a quite general context. We therefore choose a set $\mathcal{A}$ of positive integers, and we write $X = \#\mathcal{A}$. Let $\rho(d)$ be an appropriate multiplicative function, and define

$$R_d = \#\mathcal{A}_d - \frac{\rho(d)}{d} X.$$

We shall suppose that our set has 'level of distribution' D, in the sense that

$$\sum_{d \le D} \Lambda(d)|R_d| \ll X. \tag{10.1}$$

We shall also assume that there is some constant Δ such that

$$\Delta \log D + O(1) \le \log n < \Delta \log D \tag{10.2}$$

for all $n \in \mathcal{A}$. We shall take the constant Δ to be an integer, for simplicity of exposition, and we shall think of it as representing the 'degree' of the set $\mathcal{A}$. Moreover, we shall suppose that

$$\sum_{d \le x} \frac{\rho(d)}{d} \Lambda(d) = \log x + O(1), \tag{10.3}$$

so that we have a 1-dimensional sieve.

In our setting we might choose

$$\mathcal{A} = \{n^3 + 2 : \ X < n \le 2X\}$$

and $\Delta = 3$.

Returning to the general formulation, it is immediate from (10.1) and (10.3) that

$$\sum_{\lambda D < p \le D} (\log p) \#\mathcal{A}_p = (\log \lambda^{-1}) X + O(X).$$

Thus, if λ is a sufficiently small constant, there must exist $n \in \mathcal{A}$ with a divisor $p > \lambda D$. We shall regard this as the trivial result.

To get a non-trivial result the standard method is as follows. For any positive integer n, define

$$\log^{(1)} n = \sum_{d|n,\, d\le D} \Lambda(d).$$

Then

$$\begin{aligned}\sum_{n\in\mathcal{A}} \log^{(1)} n &= \sum_{d\le D} \Lambda(d)\#\mathcal{A}_d \\ &= X\sum_{d\le D}\frac{\rho(d)}{d}\Lambda(d) + O(X) \\ &= X\log D + O(X), \end{aligned} \tag{10.4}$$

by (10.1) and (10.3). One now chooses a constant $\theta > 1$ and decomposes $\log n$ as

$$\begin{aligned}\log n &= \sum_{d|n,\, d\le D}\Lambda(d) + \sum_{d|n,\, D<d\le D^\theta}\Lambda(d) + \sum_{d|n,\, d>D^\theta}\Lambda(d) \\ &= \log^{(1)} n + \log^{(2)} n + \log^{(3)} n,\end{aligned}$$

say. In general one then tries to show that

$$\begin{aligned}\sum_{n\in\mathcal{A}} \log^{(2)} n &= \sum_{D<d\le D^\theta}\Lambda(d)\#\mathcal{A}_d \\ &\le (\Delta - 1 - \delta)X\log D \end{aligned} \tag{10.5}$$

for large enough X, if the constant $\delta > 0$ is chosen suitably. A comparison of (10.2), (10.4) and (10.5) then reveals that

$$\begin{aligned}\sum_{n\in\mathcal{A}} \log^{(3)} n &= \sum_{n\in\mathcal{A}} (\log n - \log^{(1)} n - \log^{(2)} n) \\ &\ge X\Delta\log D - X\log D - O(X) - (\Delta - 1 - \delta)X\log D \\ &= \delta X\log D + O(X).\end{aligned}$$

Thus there is an $n \in \mathcal{A}$ with a divisor $p^e > D^\theta$. Under suitable circumstances one can show that the exponent e may be taken to be 1, giving a result of the desired type. Clearly this approach therefore hinges on the availabilty of upper bound information on $\#\mathcal{A}_p$ for $D < p \le D^\theta$ so that (10.5) can be established.

We now describe our alternative approach, again in the general setting. We should note that the function $\log^{(1)}$ defined above does not correspond exactly to that used in §2, since the condition $d \le D$ does not correspond exactly to $\Lambda(d) \le \log D$. However, when d is a prime the two conditions agree, and this is the most important case.

The key idea is to construct a set $\mathcal{A}^{(1)} \subseteq \mathcal{A}$, of cardinality $X_1 \gg X$, with the property that

$$\log^{(1)} n \ge (1+\delta)\log D \quad \text{for all} \quad n \in \mathcal{A}^{(1)}. \tag{10.6}$$

Now suppose that the set $\mathcal{A} \setminus \mathcal{A}^{(1)}$ contains precisely X_2 elements n with $\log^{(1)} n \ge (1-\delta')\log D$, where δ' is to be chosen later. It then follows that

$$\sum_{n\in\mathcal{A}} \log^{(1)} n \ge X_1(1+\delta)\log D + X_2(1-\delta')\log D,$$

whence (10.4) yields

$$X_1(1+\delta) + X_2(1-\delta') \le X + O(\frac{X}{\log D}).$$

Now, if we set

$$\mathcal{A}^{(3)} = \{n \in \mathcal{A} : \log^{(1)} n < (1-\delta')\log D\}$$

and $X_3 = \#\mathcal{A}^{(3)} = X - X_1 - X_2$, we deduce that

$$X_1(1+\delta) + (X - X_1 - X_3)(1-\delta') \le X + O(\frac{X}{\log D}),$$

whence

$$X_3 \ge X_3(1-\delta') \ge X_1(\delta+\delta') - X\delta' + O(\frac{X}{\log D}).$$

We shall therefore choose

$$\delta' = \delta\frac{X_1}{X},$$

whence

$$X_3 \ge \delta(\frac{X_1}{X})^2 X + O(\frac{X}{\log D}).$$

In view of (10.2) we have

$$\sum_{d|n,\, d>D} \Lambda(d) > (\Delta - 1 + \delta')\log D + O(1)$$

for any $n \in \mathcal{A}^{(3)}$. We shall suppose that

$$\#\{n \in \mathcal{A} : \exists p^e | n,\, p^e \ge D,\, e \ge 2\} \ll \frac{X}{\log D}.$$

Moreover we define

$$\mathcal{A}^{(4)} = \{n \in \mathcal{A} : \sum_{p|n,\, d>D} \log p > (\Delta - 1 + \delta')\log D\}$$

and $X_4 = \#\mathcal{A}^{(4)}$. It then follows that

$$X_4 \ge \delta(\frac{X_1}{X})^2 X + O(\frac{X}{\log D}).$$

However it is clear from (10.2) that any $n \in \mathcal{A}^{(4)}$ can have at most $\Delta - 1$ prime factors $p > D$. It follows that there must be at least one prime factor p with

$$\log p \ge \frac{\Delta - 1 + \delta'}{\Delta - 1}\log D,$$

or, equivalently,

$$p \ge D^\theta, \quad \theta = 1 + \frac{\delta'}{\Delta - 1}.$$

This is the desired conclusion. Clearly, this second approach requires us to construct a set of integers n, each with a 'D-smooth' factor $d \ge D^{1+\delta}$, so that $\log^{(1)} n \ge (1+\delta)\log D$.

We should stress that neither of these two approaches will work without detailed knowledge of the set $\mathcal{A}$. However it is worth emphasizing that the second approach allows us considerable freedom in constructing $\mathcal{A}^{(1)}$, whereas the first approach requires us to consider $\mathcal{A}_p$ specifically for primes p.

We shall now discuss in a little more detail the arguments leading to (10.5) and (10.6) for our particular set $\mathcal{A}$. One can produce an estimate of the type given in (10.5) by using an upper bound sieve method. For example, suppose that one can show

$$\sum_{P<p\le 2P} \#\mathcal{A}_p \le \{C+o(1)\}X \sum_{P<p\le 2P} p^{-1}, \tag{10.7}$$

for some constant C, and any P with $D \ll P \ll D^\theta$. Then we will be able to deduce (10.5) for any $\theta < 1 + C^{-1}(\Delta - 1)$, providing that the prime powers can be satisfactorily handled. To achieve a bound of the form (10.7) one needs information about

$$\sum_{m:\, P<dm\le 2P} R_{dm} \tag{10.8}$$

for values of d up to some small level of distribution. For the particular set $\mathcal{A} = \{n^3+2 :\ X < n \le 2X\}$, Hooley was able to handle this problem, but only under Hypothesis R*.

In order to examine Hooley's analysis it will be simplest if we depart considerably from Hooley's exposition, and indeed from the above formulation, and work with the set

$$\mathcal{A} = \{n + \sqrt[3]{2} :\ X < n \le 2X\}.$$

We then see that in place of (10.8) we must handle

$$\sum_{I:\, P<N(BI)\le 2P} R_{BI}$$

where $N(B)$ is 'small' and $D \ll P \ll D^\theta$. In particular, a simple estimate with level of distribution D is insufficient.

In contrast, our new approach requires information about sums of the form

$$\sum_{J\in\mathcal{J}:\, Q<N(J)\le 2Q} R_J, \tag{10.9}$$

where $\mathcal{J}$ is a set of 'D-smooth' ideals.

In view of Lemma 4 one needs, in either case, a non-trivial bound for the exponential sum $\sigma(n)$. In both methods one fixes a and b, and hence q, and sums over c, which is essentially of order $q^{1/3}$. In Hooley's analysis there is no control over q, and one must resort to Hypothesis R* in order to get a suitable estimate for $\sigma(n)$.

In contrast the new approach allows us considerable freedom in choosing the ideals J in (10.9). We may therefore restrict the set $\mathcal{J}$ so that the modulus q factorizes sufficiently well for Theorem 2 to apply. This is the key to our success.

References

[1] J.-M. Deshouillers and H. Iwaniec, On the greatest prime factor of n^2+1, *Ann. Inst. Fourier (Grenoble),* 32 (1982), *no.* 4, 1-11 (1983).

[2] P. Erdős, On the greatest prime factor of $\prod f(k)$, *J. London Math. Soc.,* 27 (1952), 379-384.

[3] G.R.H. Greaves, Large prime factors of binary forms, *J. Number Theory,* 3 (1971), 35-59.

[4] D.R. Heath-Brown, Hybrid bounds for L-functions: a q-analogue of van der Corput's method and a t-analogue of Burgess's method, *Recent progress in analytic number theory,* (Academic Press, London, 1981), 121-126.

[5] C. Hooley, On the greatest prime factor of a quadratic polynomial, *Acta Math.,* 117 (1967), 281-299.

[6] C. Hooley, On the greatest prime factor of a cubic polynomial, *J. reine angew. Math.,* 303/304 (1978), 21-50.

[7] H. Iwaniec, Rosser's sieve, *Acta Arith.,* 36 (1980), 171-202.

[8] A.A. Markov, Über die Primteiler der Zahlen von der Form $1 + 4x^2$, *Bull. Acad. Sci. St. Petersburg,* 3 (1895), 55-59.

[9] T. Nagell, Généralisation d'un theorème de Tchebycheff, *J. Math. Pures Appl.,* 4 (1921), 343-356.

[10] G. Tenenbaum, Sur une question d'Erdős et Schinzel, *Invent. Math.,* 99 (1990), 215-224.

[11] E.C. Titchmarsh, *The theory of the Riemann Zeta-function,* (Clarendon Press, Oxford,1986).