The Solubility of Diagonal Cubic Diophantine Equations

D.R. Heath-Brown
Magdalen College, Oxford

1 Introduction

This paper is concerned with the following question: Which Diophantine equations

$$\sum_{i=1}^{n} a_i X_i^3 = 0 \quad (a_i \in \mathbb{Z} \setminus \{0\}) \tag{1}$$

have non-zero integer solutions? For large values of n the issue may be settled by the Hardy-Littlewood circle method. Thus for $n \geq 9$ the methods of Hardy and Littlewood [11] suffice to show that solutions necessarily exist. Indeed their techniques permit one to establish an asymptotic formula for the number of solutions in a large cube $|X_i| \leq P$, the main term taking the form cP^{n-3} with a positive constant c. When $n = 8$ the existence of solutions follows immediately from the method of Davenport [7], as was first remarked by Davenport and Lewis [8]. The proof of the corresponding asymptotic formula is distinctly harder however, and is due to Vaughan [20]. The existence problem for $n = 7$ was solved by Baker [1] using methods of Vaughan [20]. However the asymptotic formula in this case remains to be established. None the less it seems likely that ideas of Vaughan [21] would lead to a lower bound of the correct order of magnitude. Moreover Hooley [12] has given a conditional approach, requiring the analytic continuation and Riemann hypothesis for Hasse-Weil L-functions of certain cubic 3-folds, which would yield the expected asymptotic formula.

For smaller values of n there are few unconditional existence results of substance. It should be stresssed that for $n \geq 7$ the equation (1) always has non-zero solutions in every p-adic field, by a result of Lewis [13]. However, even for $n = 6$ this is no longer true, as one sees from the example

$$(x_1^3 - kx_2^3) + p(x_3^3 - kx_4^3) + p^2(x_5^3 - kx_6^3) = 0,$$

where $p \equiv 1 \pmod 6$ is a prime, and k is a cubic non-residue of p. Thus for $n \leq 6$ one may ask whether there is a Hasse Principle; that is to say, whether (1) has non-zero integer solutions whenever it has such solutions in every p-adic

field. This is indeed conjectured to be the case when $n = 5$ or 6, but for $n = 3$ and 4 there are well known counterexamples, including the equations

$$3x_1^3 + 4x_2^3 + 5x_3^3 = 0$$

and

$$5x_1^3 + 9x_2^3 + 10x_3^3 + 12x_4^3 = 0$$

of Selmer [17], and Cassels and Guy [5], respectively. All known examples of this type are explained by the Manin obstruction. For our particular problem, in the case $n = 4$, the reader is referred to the comprehensive treatment of the Manin obstruction given by Colliot-Thélène, Kanevsky and Sansuc [6]. Of special relevence to us will be the corollary to Proposition 2 of [6], which states that, for equation (1) with $n = 4$ and cube-free coefficients a_i, the Manin obstruction is empty unless every prime factor of $a_1a_2a_3a_4$ divides at least two of the coefficients a_i. In particular the Manin obstruction is empty when $a_1a_2a_3a_4$ is square-free.

For $n = 3$ the curve (1) has genus 1, and the theory of elliptic curves can be brought to bear on the problem. None the less there are very few unconditional results predicting the existence of solutions. A notable example is Proposition 3.3 of Satgé [15], which shows that

$$X_1^3 + 2X_2^3 + pX_3^3 = 0$$

has non-zero integer solutions for every prime $p \equiv 2 \pmod 9$. Conditionally however the situation for $n = 3$ is well understood. In particular Manin [14] has shown that the Manin obstruction is the only obstruction to the Hasse principle, providing that the Tate-Shafarevich group is finite.

The aim of this paper is to make some modest progress with the cases $n = 4$ and $n = 5$. In order to describe our results we introduce a little nomeclature. We shall make use of properties of the rational elliptic curves

$$E(A): \ X^3 + Y^3 = A.$$

We shall denote the arithmetic rank of this curve by $r(A)$, and its analytic rank by $R(A)$. The latter is the order of vanishing of the associated L-function, $L_{E(A)}(s)$, at the point $s = 1$. This L-function is essentially a Hecke L-function with Grossencharacters. Specifically we have

$$L_{E(A)}(s - \frac{1}{2}) = L(s; A) = \sum_{\alpha \in \mathbb{Z}[\omega]}^{*} (\frac{A}{\alpha})_3 \frac{\overline{\alpha}}{|\alpha|} N(\alpha)^{-s},$$

where ω is a primitive cube root of 1, and Σ^* indicates that α is restricted to the congruence class 1 (mod 3). We shall also use the 'Selmer rank' $s(A)$, which will be described more fully in §2. It will be convenient to record the following relations between these ranks. We have

$$r(A) \leq s(A) \tag{2}$$

as the descent process shows, and

$$R(A) \equiv s(A) \pmod 2 \tag{3}$$

as was shown in this particular case by Stephens [18]. We also have

$$r(A) \geq 1 \text{ if } R(A) = 1, \tag{4}$$

by the result of Gross and Zagier [10], since $E(A)$ is modular.

Our first result depends on the following well-known conjecture.

Hypothesis 1 (Selmer Conjecture.) *We have* $r(A) \equiv s(A) \pmod 2$.

According to (3) this is equivalent to the assertion that $r(A) \equiv R(A) \pmod 2$. It is known (Cassels [4]) that the Selmer Conjecture holds providing that the Tate-Shafarevich group is finite.

We may now state our first result.

Theorem 1 *Let* $p_1, p_2, p_3, p_4 \equiv 2 \pmod 3$ *be primes. Then*

$$\sum_{i=1}^{4} p_i X_i^3 = 0$$

has non-zero integral solutions, providing that the Selmer Conjecture holds.

There are a variety of weakenings of the Selmer Conjecture that would suffice, for example one need only require that $r(A) = 1$ whenever $s(A) = 1$. Moreover there are various rather different conditions under which the conclusion of Theorem 1 holds. Thus, for example, we have the following.

Hypothesis 2 (Triple Zeros Conjecture.) *For a fixed integer* A *the number of primes* $p \leq N$ *for which* $R(Ap) \geq 3$ *is* $o(N/logN)$ *as* $N \to \infty$.

(It should be observed that this is a conjecture whose plausibility is not universally accepted!)

Theorem 2 *Let* $p_1, p_2, p_3, p_4 \equiv 2 \pmod 3$ *be primes. Then*

$$\sum_{i=1}^{4} p_i X_i^3 = 0$$

has non-zero integral solutions, providing that the Triple Zeros Conjecture holds.

It is easy to verify that the equations in Theorems 1 and 2 are everywhere locally solvable, and as remarked above, there is no Manin obstruction.

Turning to equations in 5 variables, we are able to establish the existence of solutions, for appropriate sets of coefficients, subject to a suitable form of the

Riemann Hypothesis. In addition to using the Hecke L-functions $L(s;A)$ we shall need the L-functions

$$L(s,\chi,\mathbb{Q}[\omega]) = \sum_{\alpha\in\mathbb{Z}[\omega]}{}^{*}\chi(\alpha)N(\alpha)^{-s},$$

where $\chi(\alpha)$ is a multiplicative character for $\mathbb{Q}[\omega]$. We now introduce the following hypothesis.

Hypothesis 3 (Riemann Hypothesis.) *For every A, all non-trivial zeros of $L(s;A)$, and all non-trivial zeros of $L(s,\chi,\mathbb{Q}[\omega])$, lie on the critical line $\Re(s) = \frac{1}{2}$.*

This enables us to state our next result.

Theorem 3 *Let $p_1,p_2,p_3,p_4,p_5 \equiv 8 \pmod 9$ be primes. Then*

$$\sum_{i=1}^{5} p_i X_i^3 = 0 \tag{5}$$

has non-zero integral solutions, providing that the Riemann Hypothesis, in the form given by Hypothesis 3, holds.

In fact we come very close to handling the case $n = 4$ under the Riemann Hypothesis, as will be apparent from the analysis of §3. We should point out that the necessary local conditions are automatically satisfied in Theorem 3, as is easily verified.

It is disappointing that the above results should require such restrictive conditions on the coefficients. In fact the above statements should be regarded as representative samples. Other variants may be proved, although the techniques of the present paper require severe restrictions of the prime factors of the coefficents a_i in (1). Our basic method, as described in §2, involves the use of 'first descents' only. It is conceivable that an approach which used second descents might radically reduce the constraints which have to be imposed on the coefficients. However we shall see, in §2, that one cannot hope to extend Theorem 1, for example, to all surfaces (1) for which one expects there to be rational points. Even for 5 variables we are unable to prove the Hasse Principle under any reasonable set of hypotheses. However with relatively mild conditions we can establish a worthwhile result by introducing the following restricted version of Schinzel's Hypothesis [16].

Hypothesis 4 (Schinzel's Hypothesis.) *Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be an irreducible binary cubic form. Suppose that Q_1 and Q_2 are positive integers, and that $x_0,y_0 \in \mathbb{Z}$ are such that $Q_1 | F(x_0,y_0)$. Suppose moreover that for every prime p there exist integers x_p,y_p with $p \nmid G(x_p,y_p)$, where*

$$G(X,Y) = Q_1^{-1}F(x_0 + Q_1Q_2X, y_0 + Q_1Q_2Y).$$

Then $G(m,n)$ takes infinitely many (positive) prime values for $m,n \in \mathbb{Z}$.

It is easy to see that the only primes p for which the condition might fail are those dividing $2Q_1Q_2$, and those for which $F(X,Y)$ vanishes modulo p.

We can now state our conditional version of the Hasse Principle for diagonal cubic 3-folds.

Theorem 4 *Suppose that a_1, a_2, a_3, a_4, a_5 are integers coprime to 3, and assume that none of them is divisible by the square of any prime $p \equiv 2 \pmod 3$. Then if*

$$\sum_{i=1}^{5} a_i X_i^3 = 0$$

has non-zero p-adic solutions for every prime p, it will have non-zero integral solutions, providing that both the Selmer Conjecture and Schinzel's Hypothesis, in the form given by Hypothesis 4, hold.

Although the prime 3 causes some problems, it is principally difficulties connected with the primes $p \equiv 2 \pmod 3$ which currently prevent us from proving a version of Theorem 4 applicable to all diagonal cubic 3-folds.

The idea of using the Selmer Conjecture in questions of this type is not new, but comes from the work of Swinnerton-Dyer [19] on intersections of two quadrics. However it would appear that Theorems 1-3 are the first results of this type in which an appeal to Schinzel's Hypothesis has been avoided. In fact it is necessary to use information on the representation of primes by polynomials, but fortunately only linear polynomials occur! The underlying idea for the proof of Theorem 1 is rather similar to that commonly used to handle the Hasse Principle for diagonal quadratic forms in 4 variables. Thus we shall establish a solubility criterion for the case $n = 3$ and choose a prime p such that both equations

$$p_1 X_1^3 + p_2 X_2^3 = p, \quad p_3 X_3^3 + p_4 X_4^3 = p$$

have rational solutions. The existence of a suitable p will follow from Dirichlet's theorem on primes in arithmetic progressions, for $\mathbb{Z}[\omega]$.

2 The Proofs of Theorems 1 and 2

Excellent descriptions of the first descent on $E(A)$, via multiplication by $\sqrt{-3}$, may be found in Selmer [17] and Cassels [1], and we shall content ourselves with an abstraction of the key results. Following Cassels we shall work over $\mathbb{Q}[\omega]$. It will be convenient to write $k = \mathbb{Q}[\omega]$ and

$$G = k^\times / (k^\times)^3.$$

In what follows we shall assume that $A \in \mathbb{Z} \setminus \{-1, 0, 1\}$ is cube-free. For any coset αG we write $C(\alpha, A)$ for the set of projective curves $\beta X^3 + \beta^{-1} Y^3 = A$, with $\beta \in \alpha G$, and we observe that if any of these curves has k-rational points,

then they all will. We shall then merely say that $C(\alpha, A)$ has k-rational points. A similar convention will apply to points in a completion k_π. We may now quote the necessary results on the first descent as follows.

Lemma 1 *Let $C(A)$ be the set of cosets αG for which $C(\alpha, A)$ has k-rational points, and let $S(A)$ be the set of αG for which $C(\alpha, A)$ has k_π-rational points for every prime π of k. Then $C(A)$ and $S(A)$ are groups, with $C(A) \leq S(A)$. Moreover $\#C(A) = 3^{1+r(A)}$ and $\#S(A) = 3^{1+s(A)}$.*

We should note that the final assertion is merely the definition of $s(A)$, and that (2) is an immediate consequence of the lemma. We should also point out that the cosets of $1, A$ and A^{-1} are trivially in $C(A)$.

The observation which is the key to our results is that if $s(A) = 1$ then, according to (2) and the Selmer Conjecture, we must have $r(A) = 1$, and hence $C(A) = S(A)$. This provides a local-to-global principle for the curves $C(\alpha, A)$. Our task is thus to construct examples with $s(A) = 1$.

We may immediately note that $C(\alpha, A)$ automatically has points in k_π for any prime $\pi \not| 3A$. Moreover if $\alpha \in \mathbb{Z}[\omega]$ is a cube-free integer, divisible by any prime $\pi \not| A$, then $C(\alpha, A)$ does not have points in k_π. We may therefore restrict attention to integers α composed entirely of primes dividing A. Since $\langle A \rangle \in S(A)$ it will suffice to test coset representatives of $G/\langle A \rangle$ for membership of $S(A)$. We may do this by selecting a prime factor π_0 of A and considering only those α not divisible by π_0. A further useful general observation is that, if $A \equiv 4$ or $7 \pmod 9$, then, for integers $\alpha \in \mathbb{Z}[\omega]$ coprime to 3, the equations $C(\alpha, A)$ have no points over $k_{\sqrt{-3}}$ unless $\alpha \equiv \pm 1 \pmod 3$. Since we are only concerned with values of α modulo cubes, we may then assume that we have $\alpha \equiv 1 \pmod 3$.

In order to prove Theorem 1 we take $A = p_1 p_2 p$ where $p_1, p_2, p \in \mathbb{N}$ are primes, with $p_1 \equiv p_2 \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 3$. We shall choose p so that $A \equiv 4$ or $7 \pmod 9$ and we factor p in $\mathbb{Z}[\omega]$ as $\pi\overline{\pi}$ with $\pi \equiv 1 \pmod 3$. Providing that we have

$$\left(\frac{\pi}{p_1}\right)_3 = \left(\frac{\pi}{p_2}\right)_3 \neq 1$$

it is then easy to check that $S(A)$ is generated by the cosets of A and $p_1 p_2^{-1}$. Thus $s(A) = 1$, as required. If we also have $r(A) = 1$ we then deduce, as above, that $S(A) = C(A)$, so that

$$p_1 p_2^{-1} X^3 + p_2 p_1^{-1} Y^3 = p_1 p_2 p$$

has a k-rational point. Since this curve is defined over $\mathbb{Q}$, and k is a quadratic extension of $\mathbb{Q}$, there is a $\mathbb{Q}$-rational point (x, y), say. We then deduce that

$$p_1 \left(\frac{y}{p_1}\right)^3 + p_2 \left(\frac{x}{p_2}\right)^3 = p,$$

which leads to the following result.

Lemma 2 *Let $p_1, p_2, \in \mathbb{N}$ be primes, with $p_1 \equiv p_2 \equiv 2 \pmod 3$. Suppose that $\pi \in \mathbb{Z}[\omega]$ is a prime with $\pi \equiv 1 \pmod 3$ and that $A \not\equiv 1 \pmod 9$, where $A = p_1 p_2 N(\pi)$. Assume further that*

$$(\frac{\pi}{p_1})_3 = (\frac{\pi}{p_2})_3 \neq 1.$$

Then $s(A) = 1$, and there are $\mathbb{Q}$-rational points on

$$p_1 X^3 + p_2 Y^3 = N(\pi),$$

providing that $r(A)$ is also 1.

Certainly the Selmer Conjecture is enough to ensure that $r(A) = 1$, so it suffices for the proof of Theorem 1 to choose $\pi \equiv 1 \pmod 3$ so that

$$p_1 p_2 N(\pi) \not\equiv 1 \pmod 9, \tag{6}$$

$$p_3 p_4 N(\pi) \not\equiv 1 \pmod 9, \tag{7}$$

and

$$(\frac{\pi}{p_1})_3 = (\frac{\pi}{p_2})_3 = (\frac{\pi}{p_3})_3 = (\frac{\pi}{p_4})_3 \neq 1. \tag{8}$$

We therefore choose $B = 1, 4$ or 7 so that

$$p_1 p_2 B \not\equiv 1 \pmod 9 \quad \text{and} \quad p_3 p_4 B \not\equiv 1 \pmod 9,$$

whence (6) and (7) will hold if $N(\pi) \equiv B \pmod 9$. We arrrange this by taking $\pi \equiv 1, -2$ or $1 + 3\omega \pmod 9$ respectively. The conditions (8) may be satisfied by taking π to belong to a suitable congruence class $\pmod{p_1 p_2 p_3 p_4}$. It follows from the Chinese Remainder Theorem that there exists an invertible residue class $\beta \pmod{9 p_1 p_2 p_3 p_4}$ for which the equations

$$p_1 X^3 + p_2 Y^3 = N(\pi), \quad p_3 U^3 + p_4 V^3 = N(\pi),$$

have non-trivial rational solutions whenever $\pi \equiv \beta \pmod{9 p_1 p_2 p_3 p_4}$. Such primes π necessarily exist, by Dirichlet's theorem for $\mathbb{Z}[\omega]$, and Theorem 1 follows.

The above argument only needs a few modifications in order to establish Theorem 2. The Prime Number Theorem for arithmetic progressions, in $\mathbb{Z}[\omega]$, shows that there are at least $cN/\log N$ primes $\pi \equiv \beta \pmod{9 p_1 p_2 p_3 p_4}$ in the range $N(\pi) \leq N$, if $c = c(p_1 p_2 p_3 p_4)$ is a suitable positive constant and N is large enough. According to the Triple Zeros Conjecture $o(N/\log N)$ of these can have $R(p_1 p_2 N(\pi)) \geq 3$, and similarly for $R(p_3 p_4 N(\pi))$. If N is suffciently large it follows that we can find a prime $\pi \equiv \beta \pmod{9 p_1 p_2 p_3 p_4}$ for which $R(p_1 p_2 N(\pi))$ and $R(p_3 p_4 N(\pi))$ are both at most 2. Since $s(p_1 p_2 N(\pi)) = s(p_3 p_4 N(\pi)) = 1$ we deduce from (3) that $R(p_1 p_2 N(\pi))$ and $R(p_3 p_4 N(\pi))$ are both odd, and

hence that they must both be 1. The Gross-Zagier result (4) now shows that $r(p_1p_2N(\pi))$ and $r(p_3p_4N(\pi))$ are both positive, and finally the bound (2) implies that $r(p_1p_2N(\pi)) = r(p_3p_4N(\pi)) = 1$. We can now complete the proof of Theorem 2 in exactly the same way as for Theorem 1.

We conclude this section by drawing attention to two clear limitations to the method developed here. For any cube free integer A with exactly m distinct rational prime factors $q \equiv 2 \pmod 3$, we write

$$s_0(A) = \begin{cases} m, & 3||A, \\ m-1, & 3^2||A, \\ m-1 & A \equiv \pm 4 \text{ or } \pm 7 \pmod 9, \\ m-2 & A \equiv \pm 1 \pmod 9. \end{cases}$$

One can then show that

$$s(A) \geq s_0(A), \tag{9}$$

and that $s(A) \equiv s_0(A) \pmod 2$. Now, for the approach used in the proof of Theorem 1 to work for the general case $n = 4$ of (1), we will need to find an integer h for which

$$s(a_1a_2h) = s(a_3a_4h) = 1,$$

possibly having re-numbered the coefficients. Evidently, this is doomed to failure if the a_i have too many prime factors $q \equiv 2 \pmod 3$.

By using some other type of descent argument one might hope to avoid this problem, by replacing $s(A)$ by a smaller 'Selmer Rank', $s'(A)$, say. One would then re-number the coefficients of (1), taking $n = 4$, and try to find a cube-free integer h such that

$$a_1X_1^3 + a_2X_2^3 = h \quad \text{and} \quad a_3X_3^3 + a_4X_4^3 = h \tag{10}$$

are both soluble in every completion k_π, and such that $s'(a_1a_2h)$ and $s'(a_3a_4h)$ are both equal to 1. Since we should have $s'(A) \equiv R(A) \equiv s(A) \pmod 2$ in general, as in (3), this latter condition would entail $s(a_1a_2h)$ and $s(a_3a_4h)$ being odd. Hence $s_0(a_1a_2h)$ and $s_0(a_3a_4h)$ would also have to be odd. In general, and in particular for the example

$$X_1^3 + 3X_2^3 + 7X_3^3 + 67X_4^3 = 0,$$

this cannot be achieved. This surface does indeed have rational points, such as $(2, 1, 2, -1)$. Suppose however that we label the coefficients with $a_1 = 3$, and assume that both curves (10) have points in $k_{\sqrt{-3}}$. Then we readily find that either $3||h$ or $h \equiv \pm a_3$ or $\pm a_4 \pmod 9$. If h has exactly m distinct rational prime factors $q \equiv 2 \pmod 3$, we then find that

$$s_0(a_1a_2h) = m - 1, \quad s_0(a_3a_4h) = m,$$

for $3||h$ and

$$s_0(a_1a_2h) = m, \quad s_0(a_3a_4h) = m - 1,$$

for $h \equiv \pm a_3$ or $\pm a_4 \pmod 9$. It therefore follows that we cannot arrange for both values to be odd, and the method fails.

3 Proof of Theorem 3

To establish Theorem 3 we shall find a prime $\pi \in \mathbb{Z}[\omega]$ such that $\pi \equiv 4 \pmod 9$, so that $N(\pi) \equiv 7 \pmod 9$, and for which

$$(\frac{\pi}{p_1})_3 = (\frac{\pi}{p_2})_3 = (\frac{\pi}{p_3})_3 = (\frac{\pi}{p_4})_3 = (\frac{\pi}{p_5})_3 \neq 1.$$

If $Q = 9p_1p_2p_3p_4p_5$ and ρ is appropriately chosen, with $(\rho, Q) = 1$, then π will fulfill the above conditions whenever it lies in the congruence class $\rho \pmod Q$. Then, providing that there are 4 distinct indices i, j, k, l such that

$$R(p_ip_jN(\pi)) = R(p_kp_lN(\pi)) = 1 \tag{11}$$

we shall be able to mimic the proof of Theorem 2 to obtain solutions of

$$p_iX^3 + p_jY^3 = p_kU^3 + p_lV^3 = N(\pi). \tag{12}$$

This clearly provides a solution of the original equation (5), with one of the variables being zero.

We shall establish the following result.

Lemma 3 *Assume the Riemann Hypothesis in the form given by Hypothesis 3. Then for fixed Q, and a fixed cube-free $A \in \mathbb{N}$, we have*

$$\sum_{\substack{N(\pi)\leq T \\ \pi\equiv\rho(\mathrm{mod}\ Q)}} R(AN(\pi)) \leq (2 + o(1)) \sum_{\substack{N(\pi)\leq T \\ \pi\equiv\rho(\mathrm{mod}\ Q)}} 1, \tag{13}$$

as $T \to \infty$.

One may view this as a substitute for the Triple Zeros Conjecture. Unfortunately it appears to be (just) insufficient to handle the case $n = 4$. For the latter purpose it would suffice to have the factor $2 + o(1)$ on the right hand-side replaced by $2 - \delta + o(1)$, for any constant $\delta > 0$.

We proceed to demonstrate how Theorem 3 follows from Lemma 3. As before, the congruence conditions imposed on π show that $s(p_ip_jN(\pi)) = 1$ for ever pair i, j, and hence, by (3) that $R(p_ip_jN(\pi))$ must be odd. We now consider the complete graph on 5 vertices, labeled $1, 2, 3, 4, 5$, and mark those edges $\{i, j\}$ for which $R(p_ip_jN(\pi)) = 1$. If there are not two disjoint pairs i, j and k, l for which (11) holds, then the marked edges must either form a triangle, or must be concurrent. Thus there can be at most 4 such edges. Thus π will provide a solution to (12), unless at most 4 pairs i, j have $R(p_ip_jN(\pi)) = 1$. In

the remaining case all other pairs k, l will have $R(p_k p_l N(\pi)) \geq 3$. We would then have

$$\sum_{i<j} R(p_i p_j N(\pi)) \geq 4 + 6 \times 3 = 22.$$

If there is no suitable π in the range $N(\pi) \leq T$ we therefore conclude that

$$\sum_{\substack{N(\pi)\leq T \\ \pi \equiv \rho (\mathrm{mod}\ Q)}} \sum_{i<j} R(p_i p_j N(\pi)) \geq 22 \sum_{\substack{N(\pi)\leq T \\ \pi \equiv \rho (\mathrm{mod}\ Q)}} 1,$$

whence there is some pair i, j for which

$$\sum_{\substack{N(\pi)\leq T \\ \pi \equiv \rho (\mathrm{mod}\ Q)}} R(p_i p_j N(\pi)) \geq \frac{22}{10} \sum_{\substack{N(\pi)\leq T \\ \pi \equiv \rho (\mathrm{mod}\ Q)}} 1.$$

This contradicts Lemma 3 if T is large enough, thereby establishing Theorem 3.

We may observe at this point that the corresponding argument for $n = 4$ only fails if for 'almost-all' relevent primes π, and every partition of $\{1, 2, 3, 4\}$ into pairs $\{i, j\}$ and $\{k, l\}$, one of the ranks $R(p_i p_j N(\pi))$, $R(p_k p_l N(\pi))$ is 1 and the other is 3. In this case we will have equality in (13), which, as we shall see, would require a remarkable configuration of the zeros of the functions $L(s; AN(\pi))$.

Our treatment of Lemma 3 is based on the approach developed by Goldfeld [9] and Brumer [2] for estimating the average analytic rank of elliptic curves. We take as our starting point Proposition 2.9 of Brumer [2], which we state below in a slightly more precise form. First we must introduce a little notation. Let h be an even continuous function of compact support contained in $[-1, 1]$. We suppose further that $h(x)$ is bounded and has piecewise continuous derivative, and we write

$$\hat{h}(x) = \int_{-\infty}^{\infty} e^{-iux} h(u) du.$$

Let E be a modular elliptic curve of conductor N_E, and write its non-trivial zeros as $1 + i\tau$, so that τ is real if the appropriate Riemann Hypothesis holds. If the Euler factors of $L_E(s)$ are

$$(1 - a_p(E) p^{-s} + p^{1-2s})^{-1}$$

for primes $p \not| N_E$ we set

$$S_j(E; X) = \sum_{\substack{p^j \leq X \\ p \not| N_E}} \frac{a_p(E)^j}{p^j} h(\frac{\log p^j}{\log X}) \log p, \quad (j = 1, 2)$$

for any $X \geq 2$. We may then state Proposition 2.9 of Brumer [2] as follows.

Lemma 4 *Suppose all non-trivial zeros of the L-function $L_E(s)$ lie on the critical line $\Re(s) = 1$. Then*

$$\sum_{\tau} \hat{h}(\tau \log X) = h(0)\frac{\log N_E}{\log X} + \hat{h}(0) - \frac{2}{\log X}(S_1(E;X) + S_2(E;X)) + O((\log N_E)^{1/2}(\log X)^{-1}),$$

with the order constant depending only on the function h. In the sum on the left, zeros are counted according to multiplicity.

We shall take $h(x) = 1 - |x|$ for $|x| \leq 1$ and $h(x) = 0$ otherwise, so that

$$\hat{h}(u) = (\frac{\sin(u/2)}{u/2})^2.$$

The curves $E(A)$ are modular for cube-free $A \in \mathbb{N}$, and have conductor $3A_0^2$, where $A_0 \in \mathbb{N}$ is the conductor of the character

$$\alpha \mapsto \omega^j(\frac{A}{\alpha})_3, \quad \text{for } \alpha \equiv \omega^j \pmod 3.$$

Taking $E = E(AN(\pi))$ we therefore deduce that

$$\sum_{\gamma} \hat{h}(\gamma \log X) = 2\frac{\log N(\pi)}{\log X} + \hat{h}(0) - \frac{2}{\log X}(S_1(E;X) + S_2(E;X)) + O_A((\log N(\pi))^{1/2}(\log X)^{-1}),$$

where the non-trivial zeros of $L(s; AN(\pi))$ are $\frac{1}{2} + i\gamma$, counted according to multiplicity. In our context we have

$$a_p(E(A)) = \overline{\nu}(\frac{A}{\nu})_3 + \overline{\nu(\frac{A}{\nu})_3}$$

if $p \nmid 3A$ and $p = N(\nu)$ with $\nu \equiv 1 \pmod 3$. Moreover $a_p(E(A)) = 0$ for a rational prime $p \nmid 3A$ with $p \equiv 2 \pmod 3$. We may therefore reverse the argument given in (2.8) of Brumer [2], to give

$$S_2(E(A);X) = \frac{\hat{h}(0)}{2}\log X + \sum_{\substack{N(\nu) \leq \sqrt{X} \\ \nu \nmid 3A}} N(\nu)^{-2}\nu^2(\frac{A}{\nu})_3 h(\frac{\log N(\nu)^2}{\log X})\log N(\nu) + O(\log\log A),$$

where $\nu \equiv 1 \pmod 3$ runs over primes of $\mathbb{Z}[\omega]$. We therefore conclude that

$$\sum_{\gamma} \hat{h}(\gamma \log X) = 2\frac{\log N(\pi)}{\log X} - \frac{2}{\log X}(T_1(\pi; X) + T_2(\pi; X)) + O_A((\log N(\pi))^{1/2}(\log X)^{-1}), \quad (14)$$

for the non-trivial zeros $\frac{1}{2} + i\gamma$ of $L(s; AN(\pi))$, where

$$T_1(\pi; X) = \sum_{\substack{N(\nu) \le X \\ \nu \nmid 3AN(\pi)}} N(\nu)^{-1} \overline{\nu}(\frac{AN(\pi)}{\nu})_3 h(\frac{\log N(\nu)}{\log X}) \log N(\nu)$$

and

$$T_2(\pi; X) = \sum_{\substack{N(\nu) \le \sqrt{X} \\ \nu \nmid 3AN(\pi)}} N(\nu)^{-2} \nu^2 (\frac{AN(\pi)}{\nu})_3 h(\frac{\log N(\nu)^2}{\log X}) \log N(\nu).$$

Using the Riemann Hypothesis for the functions $L(s, \chi, \mathbb{Q}[\omega])$ we shall establish the following estimate.

Lemma 5 *Let $\nu \nmid Q$ be a prime of $\mathbb{Z}[\omega]$. Then*

$$\sum_{\substack{\pi \equiv \rho \pmod Q \\ N(\pi) \le T}} (\frac{N(\pi)}{\nu})_3 \ll_Q T^{1/2} (\log TN(\nu))^2.$$

For the proof, we begin by observing that

$$(\frac{N(\beta)}{\nu})_3 = (\frac{\beta}{\nu})_3 \overline{(\frac{\beta}{\overline{\nu}})_3} = \psi_1(\beta),$$

say, where ψ_1 is a character to modulus $N(\nu)$. Then

$$\sum_{\substack{\pi \equiv \rho \pmod Q \\ N(\pi) \le T}} \psi_1(\pi) = \frac{1}{\phi(Q)} \sum_{\psi \pmod Q} \overline{\psi(\rho)} \sum_{N(\pi) \le T} \psi(\pi)\psi_1(\pi), \quad (15)$$

where $\phi(Q)$ is the Euler function for $\mathbb{Z}[\omega]$, and ψ runs over all characters to modulus Q. A standard argument shows that, under the Riemann Hypothesis for $L(s, \chi, \mathbb{Q}[\omega])$ with a non-trivial character χ to modulus δ, one has

$$\sum_{N(\pi) \le T} \chi(\pi) \ll T^{1/2} (\log TN(\delta))^2.$$

We now get a bound $O(T^{1/2}(\log TQN(\nu))^2)$ for (15), since the characters $\psi\psi_1$ are all non-principal, and Lemma 5 follows.

We can now complete the proof of Lemma 3. We sum both sides of (14) over primes $\pi \equiv \rho \pmod{Q}$, with $N(\pi) \leq T$. Lemma 5 yields

$$\begin{aligned}\sum_{\substack{\pi \equiv \rho \pmod{Q} \\ N(\pi) \leq T}} T_1(\pi; X) &\ll_Q T^{1/2}(\log TX)^2 \sum_{\substack{N(\nu) \leq X \\ \nu \nmid 3AN(\pi)}} N(\nu)^{-1/2} \log N(\nu) \\ &\ll_Q (TX)^{1/2}(\log TX)^2,\end{aligned}$$

and

$$\begin{aligned}\sum_{\substack{\pi \equiv \rho \pmod{Q} \\ N(\pi) \leq T}} T_2(\pi; X) &\ll_Q T^{1/2}(\log TX)^2 \sum_{\substack{N(\nu) \leq \sqrt{X} \\ \nu \nmid 3AN(\pi)}} N(\nu)^{-1} \log N(\nu) \\ &\ll_Q T^{1/2}(\log TX)^3.\end{aligned}$$

It therefore follows that

$$\begin{aligned}\sum_{\substack{\pi \equiv \rho \pmod{Q} \\ N(\pi) \leq T}} \sum_{\gamma} \hat{h}(\gamma \log X) &= 2 \sum_{\substack{\pi \equiv \rho \pmod{Q} \\ N(\pi) \leq T}} \frac{\log N(\pi)}{\log X} \\ &+ O_{A,Q}\left(\frac{T}{\log T} \frac{(\log T)^{1/2}}{\log X}\right) + O_Q((TX)^{1/2}(\log TX)^3).\end{aligned}$$

The main term is

$$2\frac{\log T}{\log X} \sum_{\substack{\pi \equiv \rho \pmod{Q} \\ N(\pi) \leq T}} 1 + O_Q\left(\frac{T}{\log T}(\log X)^{-1}\right),$$

by the prime number theorem for arithmetic progressions, for $\mathbb{Z}[\omega]$. We choose $X = T(\log T)^{-9}$, whence the error terms are $O_{A,Q}(\frac{T}{\log T}(\log T)^{-1/2})$, and

$$2\frac{\log T}{\log X} = 2 + O\left(\frac{\log \log T}{\log T}\right).$$

This leads to the estimate

$$\sum_{\substack{\pi \equiv \rho \pmod{Q} \\ N(\pi) \leq T}} \sum_{\gamma} \hat{h}(\gamma \log X) = 2 \sum_{\substack{\pi \equiv \rho \pmod{Q} \\ N(\pi) \leq T}} 1 + O_{A,Q}\left(\frac{T}{\log T}(\log T)^{-1/2}\right). \quad (16)$$

Since $\hat{h}(t) \geq 0$ for all t, and $\hat{h}(0) = 1$, we see that the left-hand side is at least

$$\sum_{\substack{\pi \equiv \rho \pmod{Q} \\ N(\pi) \leq T}} R(AN(\pi)),$$

and Lemma 3 follows.

We conclude by observing that if the average analytic rank estimated in Lemma 3 is exactly 2, then all zeros other than $\gamma = 0$ must make a negligible contribution in (16). Thus, for 'almost all' π, and 'almost all' 'small' zeros $\frac{1}{2} + i\gamma$ of $L(s, AN(\pi))$, we would find that

$$\hat{h}(\gamma \log X) = (\frac{\sin(\frac{1}{2}\gamma \log X)}{\frac{1}{2}\gamma \log X})^2$$

is 'small', whence γ is 'close to' an integer multiple of $2\pi_0 / \log N(\pi)$. (Here π_0 is the minimal positive period of the $\sin x$ function!)

4 The Proof of Theorem 4

Our strategy in proving Theorem 4 will be to reduce (1), with $n = 5$, to an equation in 3 variables which can be handled by an extension of the method used for Theorem 1. We will begin by writing

$$\sum_{i=1}^{5} a_i X_i^3 = 0 \tag{17}$$

as

$$\sum_{i=1}^{4} a_i a_5^2 X_i^3 + (a_5 X_5)^3 = 0.$$

We may then remove any cube factors, and re-define the variables, so as to produce a new equation

$$\sum_{i=1}^{4} b_i X_i^3 + X_5^3 = 0 \tag{18}$$

with cube-free b_i. Thus, for every rational prime $p \equiv 2 \pmod 3$ we either have $\nu_p(b_i) \neq 2$ for $1 \leq i \leq 4$ (when $p \not| a_5$) or $\nu_p(b_i) \neq 1$ for $1 \leq i \leq 4$ (when $p | a_5$).

We will then use Schinzel's Hypothesis to find $x_1, \ldots, x_4 \in \mathbb{Z}$ for which the prime factorizations of

$$B_1 = b_1 x_1^3 + b_2 x_2^3 \text{ and } B_2 = b_3 x_3^3 + b_4 x_4^3$$

are sufficiently well controlled that the methods of §2 may be used (subject to the Selmer Conjecture) to produce solutions of

$$B_1Y_1^3 + B_2Y_2^3 + Y_3^3 = 0. \tag{19}$$

We shall see that, for primes $p \equiv 2 \pmod 3$, we can choose $x_1, x_2 \in \mathbb{Z}$ so that $\nu_p(B_1) = 0$ or 3. In particular this is possible even when $p|b_1b_2$. Since we may do the same for B_2 we see that p will be absent after we have removed cube factors from the coefficients of (19). This is crucial, since we need $s(B_1B_2) = 1$ for our method to work, and this implies, by (9), that B_1B_2 can contain at most 2 primes $p \equiv 2 \pmod 3$, after eliminating cube factors. It is for this reason that Theorem 4 requires our coefficients to be square-free with respect to such primes. If $\nu_p(b_1) = 1$ and $\nu_p(b_2) = 2$, for example, we cannot have $3|\nu_p(B_1)$, so that p would be contained in B_1B_2.

In contrast to the above situation, for primes $p \equiv 1 \pmod 3$ it may happen that $\nu_p(B_1)$ is never a multiple of 3. It is therefore necessary to consider equations (19) in which the B_i may contain many prime factors $p \equiv 1 \pmod 3$.

It is clear from the above discussion that we must begin by examining the equation (18) in $\mathbb{Q}_p$, for the various prime factors p of $3\prod b_i$, with a view to producing suitable values of B_1, B_2. We may suppose at the outset that the coefficients a_i in (17) are cube-free and have no common factor. It transpires that we must give a special treatment for some prime $p \equiv 1 \pmod 3$ dividing $\prod a_i$, if any such prime exists. We therefore choose one such prime p_0 and use it in converting (17) into the form (18). (This process is unnecessary if $\prod a_i$ consists entirely of primes $p \equiv 2 \pmod 3$.) We shall show that one can arrange (18) in such a way that there are integers $x_i = x_i(p_0)$ for $1 \le i \le 4$ for which

$$\nu_{p_0}(B_1), \nu_{p_0}(B_2) \equiv 0 \pmod 3, \quad \text{and} \quad \nu_{p_0}(b_3b_4^{-1}) \not\equiv 0 \pmod 3. \tag{20}$$

It will follow, in particular, that (19) has p_0-adic solutions.

To establish our claim we shall consider two cases. For convenience of notation we shall merely write ν for the p_0-adic valuation. Suppose firstly that there are three (or more) indices for which $\nu(a_i)$ is the same. We shall re-number the coefficients so that these are a_1, a_3 and a_5. Since the coefficients have no common factor, and $p_0|\prod a_i$, not all the values of $\nu(a_i)$ can be equal, and we may therefore take a_4, say, to have $\nu(a_4) \neq \nu(a_3)$. It follows that, in the equation (18), we will have $\nu(b_1) = \nu(b_3) = 0$ and $\nu(b_3b_4^{-1}) \neq 0$. If we take $x_1 = x_3 = 1$ and $x_2 = x_4 = 0$ the conditions (20) will then be satisfied.

We turn now to the case in which no three values of $\nu(a_i)$ are equal. Then we may re-number the coefficients a_i so that $\nu(a_1) = \nu(a_2)$ and $\nu(a_3) = \nu(a_5)$, but $\nu(a_4) \neq \nu(a_3)$. Since (17) is p_0-adically solvable it follows that one or other of a_1/a_2 or a_3/a_5 must be a p_0-adic cube, and we may suppose, after a further re-numbering if necessary, that the former is a cube. Thus, if $\nu = \nu(a_1)+2\nu(a_5)$, the congruence

$$p_0^{-\nu}a_1a_5^2x^3 + p_0^{-\nu}a_2a_5^2 \equiv 0 \pmod{p_0}$$

has an integer solution $x \not\equiv 0 \pmod{p_0}$. By Hensel's Lemma we can then solve

$$p_0^{-\nu} a_1 a_5^2 y^3 + p_0^{-\nu} a_2 a_5^2 \equiv p_0^{9-\nu} \pmod{p_0^{10-\nu}}.$$

The choice $x_1 = y, x_2 = 1$ now yields $3|\nu(B_1)$. Trivially the choice $x_3 = 1, x_4 = 0$ produces $\nu(B_2) = 0$, and we have also ensured that $\nu(b_3 b_4^{-1}) \not\equiv 0 \pmod 3$, as required.

We turn next to the case $p = 3$. Here we shall show that there are integers $x_1(3), \ldots, x_4(3)$ so that

$$B_1 B_2 \equiv \pm 4 \text{ or } \pm 7 \pmod 9. \tag{21}$$

Since $b_1, \ldots, b_4$ are integers not divisible by 3, one readily checks that this may be achieved by taking $(x_1(3), \ldots, x_4(3))$ as one of $(1,0,1,0)$, $(0,1,1,0)$, $(1,1,1,0)$ or $(1,-1,1,0)$. One should observe that (21) is sufficient to ensure that (19) is 3-adically solvable.

We proceed to consider the primes $p \equiv 2 \pmod 3$ dividing $\prod b_i$. It will be convenient to include $p = 2$ in this discussion, whether or not it divides $\prod b_i$. Here we assert that there exist $x_1(p), x_2(p) \in \mathbb{Z}$ with

$$\nu_p(B_1), \nu_p(B_2) = 0 \text{ or } 3. \tag{22}$$

If $p \nmid b_1$ we merely take $x_1(p) = 1, x_2(p) = 0$, and similarly if $p \nmid b_2$. Now suppose that $\nu_p(b_1) = \nu_p(b_2) = \nu$, say, where $\nu = 1$ or 2. We set $b_i' = b_i p^{-\nu}$ for $i = 1, 2$, and note that $b_1' x^3 + b_2' \equiv 0 \pmod p$ has an integral solution. If we then replace x by $x + pt$, with a suitable choice of t we can arrange that $p^{3-\nu} || b_1'(x+pt)^3 + b_2'$. We can then take $x_1(p) = x + pt$ and $x_2(p) = 1$. The argument for B_2 is similar.

Finally, for the primes $p \equiv 1 \pmod 3$, other than $p = p_0$, we show that there exist integers $x_1(p), x_2(p), x_3(p), x_4(p)$ for which

$$B_1, B_2 \neq 0, \quad \text{and (19) has a non-trivial solution in } \mathbb{Q}_p. \tag{23}$$

We begin by proving that (18) has a p-adic solution in which x_5, $b_1 x_1^3 + b_2 x_2^3$ and $b_3 x_3^3 + b_4 x_4^3$ are all non-zero. It is clear that a non-zero p-adic solution $x_1, \ldots, x_5$ exists. Suppose that x_i, say, is non-zero. Then

$$-b_i^{-1} \sum_{\substack{1 \le j \le 5 \\ j \neq i}} b_j x_j^3$$

is a non-zero cube. (We have written $b_5 = 1$ for convenience.) Thus, if we replace x_j by x_j' with $|x_j' - x_j|_p$ sufficiently small, the value will still be a non-zero cube. In this way we can firstly arrange that x_5 is non-zero, and then taking $i = 5$, that $b_1 x_1^3 + b_2 x_2^3$ and $b_3 x_3^3 + b_4 x_4^3$ are non-zero.

Having found a suitable p-adic solution to (18) we rescale the variables so that they are all p-adic integers, and we put $y_i = x_i x_5^{-1} p^\nu$ for $1 \le i \le 4$, where

$\nu = \nu_p(x_5)$. On writing $B_1' = b_1 y_1^3 + b_2 y_2^3$, and similarly for B_2', we see that B_1' and B_2' are non-zero, and that $B_1' + B_2' = p^{3\nu}$ is a non-zero cube. Thus, if we choose $x_i(p) \in \mathbb{Z}$ with $|x_i(p) - y_i|_p$ sufficiently small we will find that B_1 and B_2 are non-zero, and $B_1 + B_2$ is a non-zero p-adic cube. This proves our assertion.

When we finally choose B_1 and B_2 we shall take

$$x_i \equiv x_i(p) \,(\mathrm{mod}\, p^k), \quad (1 \le i \le 4; \;\; p | 6 \prod b_i). \tag{24}$$

Here we choose the exponent k sufficiently large that the conditions (20), (21), (22) and (23) still hold even though the B_i are constructed from the variables x_i rather than from the $x_i(p)$. Moreover, if k is large enough, the values of $\nu_p(B_1)$ and $\nu_p(B_2)$ will be independent of the choice of the various x_i. We take k to be larger than any of these values. It is covenient at this stage to remove from B_1 and B_2, all cube factors composed of primes dividing $6 \prod b_i$, writing $B_i = C_i D_i^3$ for $i = 1, 2$. Thus D_1, for example, will be the same for all solutions of (24). Let $p_1, \ldots, p_n$ be the primes which divide both $6 \prod b_i$ and $C_1 C_2$. By construction we have $p_i \equiv 1 \,(\mathrm{mod}\, 3)$. Moreover we note that p_0 is not one of these primes. We shall set

$$e_i = \nu_{p_i}(C_1), \quad f_i = \nu_{p_i}(C_2).$$

In order to arrange that $s(C_1 C_2) = 1$ we shall introduce some further prime factors into C_1 and C_2. Thus we shall take

$$C_1 = \pm q_1 \prod_{i=1}^{n} p_i^{e_i} \tag{25}$$

and

$$C_2 = \pm q_2 \prod_{i=1}^{n} p_i^{f_i} \prod_{j=1}^{n} N(\mu_j), \tag{26}$$

where $q_1, q_2 \equiv 2 \,(\mathrm{mod}\, 3)$ are rational primes, and $\mu_j \equiv 1 \,(\mathrm{mod}\, 3)$ are primes of $\mathbb{Z}[\omega]$. In choosing these primes we must bear in mind not only that we require $s(C_1 C_2) = 1$, but that (19) must be everywhere locally solvable. Our construction ensures that (19) has solutions in $\mathbb{Q}_p$ for $p = p_i$, $(1 \le i \le n)$, and for $p = 3$, so it suffices to arrange that C_1 is a cubic residue modulo μ_j for each j.

We proceed to describe the choice of the primes μ_j. In order to do this we shall choose, for each prime p_i, a prime $\pi_i \in \mathbb{Z}[\omega]$ such that $N(\pi_i) = p_i$ and $\pi_i \equiv 1 \,(\mathrm{mod}\, 3)$. We then choose the primes μ_j successively subject to the following criteria.

(i) $\mu_j \notin \mathbb{Z}$.

(ii) μ_j does not divide $6 \prod b_i$ and differs from either of μ_l and $\overline{\mu_l}$ for $1 \le l < j$.

(iii) $\mu_j \equiv 1 \pmod 9$.

(iv) $\mu_j \equiv 1 \pmod{N(\mu_l)}$ for $1 \leq l < j$.

(v) $(\frac{\mu_j}{\pi_i})_3 = 1$ for $0 \leq i \leq n$.

(vi) $(\frac{\mu_j}{\pi_i})_3 = 1$ for $1 \leq i \leq n, \ \ i \neq j$.

(vii) $(\frac{\mu_j}{\pi_j})_3 = \omega$.

(viii) $(\frac{\mu_j}{\pi_0})_3 = \omega^{-\alpha\beta}$, where $\alpha = \nu_{p_0}(b_3 b_4^{-1})$ and $\beta = \nu_{p_j}(b_3 b_4^{-1})$.

(ix) $\mu_j \equiv 1 \pmod p$ for every prime p for which $p | b_3 b_4$ but $p \notin \{p_i\}$.

Conditions (iii)-(ix) may be satisfied by requiring μ_j to lie in an appropriate residue class. Thus a suitable prime μ_j exists, by the generalization of Dirichlet's theorem on primes in arithmetic progressions.

From conditions (v) and (vi), the law of cubic reciprocity yields

$$(\frac{p_i}{\mu_j})_3 = (\frac{\pi_i}{\mu_j})_3 (\frac{\overline{\pi_i}}{\mu_j})_3 = (\frac{\mu_j}{\pi_i})_3 (\frac{\mu_j}{\overline{\pi_i}})_3 = 1$$

for $j \neq i$. Similarly conditions (v) and (vii) produce

$$(\frac{p_j}{\mu_j})_3 = \omega,$$

while (v) and (viii) lead to

$$(\frac{p_0}{\mu_j})_3 = \omega^{-\alpha\beta}.$$

In the same way, condition (ix) shows that

$$(\frac{p}{\mu_j})_3 = 1$$

for every prime $p | b_3 b_4$ other than the primes p_i. We therefore see that $b_3 b_4$ is coprime to μ_j, and that

$$(\frac{b_3 b_4^2}{\mu_j})_3 = \omega^{-\alpha^2\beta}\omega^{\beta} = 1,$$

since $3 \nmid \alpha$, by (20). If we now set $N(\mu_j) = r_j$ it therefore follows that $b_3 b_4$ is coprime to r_j and that $b_3 b_4^2$ is a cube modulo r_j. The congruence

$$b_3 x^3 + b_4 \equiv 0 \pmod{r_j}$$

is therefore solvable, so that $b_3 x^3 + b_4 = r_j k$, for suitable integers x and k. Now, if we set $y = x + t r_j$, we find that

$$b_3 y^3 + b_4 \equiv r_j (k + 3 b_3 t x^2) \pmod{r_j^2}.$$

We shall choose t so that

$$k + 3b_3tx^2 \equiv 1 \,(\mathrm{mod}\ r_j).$$

We now set $x_3(r_j) = x + tr_j$ and $x_4(r_j) = 1$, and impose the additional conditions

$$x_i \equiv x_i(r_j) \,(\mathrm{mod}\ r_j^2), \quad (i = 3, 4, \quad 1 \leq j \leq n). \tag{27}$$

These will then ensure that $r_j || C_2$, as required for (26), and also that

$$\left(\frac{C_2/r_j}{\mu_j}\right)_3 = 1. \tag{28}$$

We have also to arrange that

$$\left(\frac{C_1}{\mu_j}\right)_3 = 1. \tag{29}$$

Since $r_j \nmid b_1 b_2$ we can solve

$$b_1 x_1(r_j)^3 + b_2 x_2(r_j)^3 \equiv 1 \,(\mathrm{mod}\ r_j).$$

Thus the conditions

$$x_i \equiv x_i(r_j) \,(\mathrm{mod}\ r_j^2), \quad (i = 1, 2, \quad 1 \leq j \leq n). \tag{30}$$

suffice.

In the case in which $\prod a_i$ has no prime factors $p \equiv 2 \,(\mathrm{mod}\ 3)$, there will be no primes p_i, and no primes μ_i. Thus we shall merely arrange that C_1 and C_2 take the form $\pm q_1$ and $\pm q_2$ respectively.

We are now ready to apply Schinzel's Hypothesis. We combine the conditions (24), (27) and (30), using the Chinese Remainder Theorem, into the congruences

$$x_i \equiv x_i^{(0)} \,(\mathrm{mod}\ R), \quad (1 \leq i \leq 4).$$

Then our construction gives $C_i = E_i F_i$ for $i = 1, 2$, and all x_i in the above congruence classes, where

$$E_1 = \prod_{i=1}^{n} p_i^{e_i}$$

and

$$E_2 = \prod_{i=1}^{n} p_i^{f_i} \prod_{j=1}^{n} N(\mu_j).$$

Moreover we have ensured that $D_i^3 E_i$ divides R, for $i = 1, 2$. We shall take $F(X, Y) = b_1 X^3 + b_2 Y^3$. If this fails to be irreducible then (18) trivially has non-zero solutions. We put $x_0 = x_1^{(0)}$ and $y_0 = x_2^{(0)}$, and we take $Q_1 = D_1^3 E_1, Q_2 =$

RQ_1^{-1}. By construction we see that $Q_1^{-1}F(x_0, y_0)$ is coprime to $6\prod b_i$, whence Schinzel's Hypothesis will apply. Moreover, since $3|Q_2$, we see that the value of $G(m,n)$, as given in Schinzel's Hypothesis, is constant modulo 3. Thus if we have $G(0,0) \equiv \pm 1 \pmod 3$, we may apply the hypothesis to $\mp F(X,Y)$ and obtain infinitely many primes $\mp G(m,n) = q > 0$, all of the form $q \equiv 2 \pmod 3$. In precisely the same way we may obtain infinitely many primes $q \equiv 2 \pmod 3$ for which $B_2 = \pm D_2^3 E_2 q$.

We have now obtained values B_1, B_2 of the form given by (25) and (26), such that (19) is everywhere locally solvable, the conditions for the primes q_1 and q_2 being automatically satisfied. It remains to verify that $s(C_1C_2) = 1$. We therefore suppose that some projective curve

$$\beta X^3 + \beta^{-1} Y^3 = C_1 C_2, \tag{31}$$

where $\beta \in \mathbb{Z}[\omega]$ is cube-free, is everywhere locally solvable. As remarked in §2, we may restrict attention to integers β composed solely of primes of $\mathbb{Z}[\omega]$ which divide C_1C_2. Moreover, by (21) we have $C_1C_2 \equiv \pm 4$ or $\pm 7 \pmod 9$, so that, as also observed in §2, we may assume that $\beta \equiv 1 \pmod 3$. Since we hope to show that the Selmer group $S(C_1C_2)$ consists only of the elements

$$H = \{G,\ C_1G,\ C_2C,\ C_1C_2G\},$$

it will suffice to prove that the quotient $S(C_1C_2)/H$ is trivial. We can choose coset representatives βG for this quotient in which β is not divisible by q_1 or q_2.

By conditions (v), (vi) and (vii) we have

$$\left(\frac{\overline{\pi_i}}{\mu_j}\right)_3 = 1 \text{ for } 0 \le i \le n,$$

$$\left(\frac{\pi_i}{\mu_j}\right)_3 = 1 \text{ for } 1 \le i \le n,\ i \ne j,$$

and

$$\left(\frac{\pi_j}{\mu_j}\right)_3 = \omega.$$

Finally we note that

$$\left(\frac{\overline{\mu_j}}{\mu_j}\right)_3 = 1,$$

by the cubic reciprocity law. Thus (28) and (29) show that

$$\left(\frac{C_1C_2/\mu_j}{\mu_j}\right)_3 = 1.$$

Suppose now that π_j divides β, where $1 \le j \le n$. If $\mu_j \nmid \beta$, then (31) is not μ_j-adically solvable, since β is not a cubic residue of μ_j. Equally, if $\mu_j || \beta$, say, we get a contradiction, because

$$(\beta/\mu_j)(C_1C_2/\mu_j)^{-1}$$

is not a cubic residue of μ_j. A similar argument applies when $\mu_j^2||\beta$. It follows that $\pi_j \nmid \beta$. We can show that $\overline{\pi_j} \nmid \beta$ in the same way, by considering $\overline{\mu_j}$-adic solvability.

We therefore see that β must be composed entirely of primes μ_j and their conjugates. However, if $\mu_j|\beta$ we see that (31) has no π_j-adic solution, since β is then a cubic non-residue of π_j. Similarly, if $\overline{\mu_j}|\beta$ there is no $\overline{\pi_j}$-adic solution. It follows that $\beta = 1$, so that $S(C_1C_2) = H$, as required. This completes the proof of Theorem 4.

5 Acknowledgement

Much of this paper was written while the author was a visitor at the Isaac Newton Institute, Cambridge. The hospitality and financial support of the institute is gratefully acknowledged.

References

[1] R.C. Baker, Diagonal cubic equations, II, *Acta Arith.,* 53 (1989), 217-250.

[2] A. Brumer, The Average Rank of Elliptic Curves, I, *Invent. Math.,* 109 (1992), 445-472.

[3] J.W.S. Cassels, Arithmetic on curves of genus 1. I. On a conjecture of Selmer, *J. Reine Angew. Math.,* 202 (1959), 52-99.

[4] J.W.S. Cassels, Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung, *J. Reine Angew. Math.,* 211 (1962), 95-112

[5] J.W.S. Cassels and M.J.T. Guy, On the Hasse principle for cubic surfaces, *Mathematika,* 13 (1966), 111-120.

[6] J.-L. Colliot-Thélène, D. Kanevsky and J.-J. Sansuc, Arithmétique des surfaces cubique diagonales, *Diophantine approximation and transcendence theory, Bonn 1985, Lecture Notes in Math., 1290,* (Springer, Berlin, 1987), 1-108.

[7] H. Davenport, On Waring's problem for cubes, *Acta Math.,* 71, (1939), 123-143.

[8] H. Davenport and D.J. Lewis, Homogeneous additive equations, *Proc. Royal Soc., A,* 274 (1963), 443-460.

[9] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, *Number Theory, Carbondale, Lecture notes in Math., 751,* (Springer, Berlin, 1979), 108-118.

[10] B.H. Gross and D. Zagier, Heegner points and derivatives of L-series, *Invent. Math.*, 84 (1986), 225-320.

[11] G.H. Hardy and J.E. Littlewood, Some problems of 'Partitio Numerorum': IV. The singular series in Waring's Problem and the value of the number $G(k)$, *Math. Zeit.*, 12 (1922), 161-188.

[12] C. Hooley, On Waring's problem, *Acta Math.*, 157 (1986), 49-97.

[13] D.J. Lewis, Cubic congruences, *Michigan Math. J.*, 4 (1957), 85-95.

[14] Ju. I. Manin, Le groupe de Brauer-Grothendieck en geometrie diophantienne, *Actes du Congrés International des Mathématiciens (Nice, 1970)*, Tome I, (Gauthier-Villars, Paris, 1971), 401-411.

[15] P. Satgé, Un analogue du calcul de Heegner, *Invent. Math.*, 87 (1987), 425-439.

[16] A. Schinzel and W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.*, 4 (1958), 185-208.

[17] E.S. Selmer, The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, *Acta Math.*, 85 (1951), 203-362.

[18] N.M. Stephens, Ph. D. Thesis, Manchester, 1965.

[19] H.P.F. Swinnerton-Dyer, Rational points on certain intersections of two quadrics, *Abelian Varieties*, (Walter de Gruyter, Berlin, 1995), 273-292.

[20] R.C. Vaughan, On Waring's problem for cubes, *J. Reine Angew. Math.*, 365 (1986), 122-170.

[21] R.C. Vaughan, On Waring's problem for cubes II, *J. London Math. Soc. (2)*, 39 (1989), 205-218.