

# The size of Selmer groups for the congruent number problem, II

D.R. Heath-Brown  
Magdalen College, Oxford OX1 4AU

## 1 Introduction

A positive integer  $D$  is said to be a congruent number if  $D$  can be the common difference of a three term arithmetic progression of squares of rational numbers. Equivalently one may require that the elliptic curve

$$E_D : y^2 = x^3 - D^2x \tag{1}$$

have positive rank. As in the first paper [5] of this series we shall be interested in the distribution of the rank  $r(D)$  of these curves. Clearly one may, and we shall, restrict attention to square-free numbers  $D$ . Our results would take essentially the same form if one were to abandon this restriction, but it would still be necessary for the proofs. To estimate  $r(D)$  one may use the method of descent. We are concerned in particular with the “full 2-descent”. The number of 2-descents is the order of the Selmer group  $S^{(2)}$ . This is a power of 2, and will be a multiple of 4, on account of the rational points of order 2 on  $E_D$ . We shall therefore write  $\#S^{(2)} = 2^{2+s(D)}$ . The exponent  $s(D)$  has sometimes been referred to as the ‘Selmer rank’ of the curve  $E_D$ . Since one has the fundamental inequality

$$r(D) \leq s(D),$$

one can use information about  $s(D)$  to say something about  $r(D)$ . The principal result of the first paper of this series shows that for  $h = 1, 3, 5$  or  $7$  we have

$$\sum_{D \in S(X, h)} 2^{s(D)} \sim 3\#S(X, h),$$

as  $X \rightarrow \infty$ , where

$$S(X, h) = \{1 \leq D \leq X; D \equiv h \pmod{8}, D \text{ odd and square-free}\}.$$

It follows that

$$\frac{\#\{D \in S(X, h); r(D) \geq r\}}{\#S(X, h)} \leq 3.2^{-r} + o(1)$$

as  $X \rightarrow \infty$ , for any fixed  $r$ . In this paper we shall determine the distribution of  $s(D)$  completely, by considering averages of  $2^{ks(D)}$ .

**Theorem 1** *For  $h = 1, 3, 5$  or  $7$ , and any fixed positive integer  $k$  we have*

$$\sum_{D \in S(X, h)} 2^{ks(D)} = c_k \#S(X, h) + o_k(X)$$

as  $X \rightarrow \infty$ , where

$$c_k = \prod_{j=1}^k (1 + 2^j).$$

It is somewhat surprising that the constant  $c_k$  is independent of  $h$ , since it turns out that the distribution of  $s(D)$  follows different patterns in the cases  $h = 1$  or  $3$ , from those for the cases  $h = 5$  or  $7$ . From Theorem 1 we shall deduce the following.

**Theorem 2** *Let*

$$\lambda = \prod_{n=1}^{\infty} (1 + 2^{-n})^{-1} = \prod_{n=0}^{\infty} (1 - 2^{-2n-1}) = 0.4194 \dots,$$

and

$$d_r = \lambda \frac{2^r}{\prod_{1 \leq j \leq r} (2^j - 1)} \quad (r = 0, 1, 2, \dots).$$

*Then if  $h = 1$  or  $3$ , and  $r$  is even, or if  $h = 5$  or  $7$ , and  $r$  is odd, we have*

$$\#\{D \in S(X, h) : s(D) = r\} \sim d_r \#S(X, h),$$

as  $X \rightarrow \infty$ .

The frequencies  $d_r$  which occur in Theorem 2 arise in another context. We consider symmetric matrices with elements in the field of 2 elements, whose diagonal entries are all zero ('skew-symmetric' matrices). If we fix  $r$  and take a positive integer  $n$  with the same parity as  $r$ , then the proportion of such  $n \times n$  matrices whose rank is  $n - r$  can be shown to be

$$\frac{2^r}{\prod_{1 \leq j \leq r} (2^j - 1)} \prod_{j=n-r+1}^n (1 - 2^{-j}) \prod_{j=0}^{(n-r)/2-1} (1 - 2^{-1-2j}).$$

As  $n \rightarrow \infty$  this proportion tends to  $d_r$ . In the appendix we shall see how skew-symmetric matrices over the field of 2 elements are relevant to  $s(D)$ . However it would be nice to have a proof of Theorem 2 which made use of this connection rather than depending on the cumbersome calculations of §§6 and 7.

As will be clear from the proof of Theorem 2 we have

$$\sum_{r=0}^{\infty} d_{2r} 2^{2rk} = \sum_{r=0}^{\infty} d_{2r+1} 2^{(2r+1)k} = c_k \quad (k = 0, 1, 2, \dots).$$

In particular it follows that the equations

$$\sum_{r=0}^{\infty} x_r 2^{rk} = c_k \quad (k = 0, 1, 2, \dots),$$

even taken together with the constraints  $x_r \geq 0$ , are insufficient to determine the numbers  $x_r$ . The necessary extra information is provided by the fact that

$$s(D) \equiv 0 \pmod{2} \quad D \equiv 1 \text{ or } 3 \pmod{8},$$

$$s(D) \equiv 1 \pmod{2} \quad D \equiv 5 \text{ or } 7 \pmod{8}.$$

This parity condition, which was included as an unproved hypothesis in the first paper [5] of this series, can in fact be derived from results of Cassels [4] and Birch and Stephens [1], as noted by Birch and Swinnerton-Dyer [2; page 95]. Specifically, one can check that, in the notation of Birch and Swinnerton-Dyer, one has  $s(D) = \lambda^* + \lambda_1 - 2$ . Using the work of Cassels [4] one may show that  $\lambda^*$  has the same parity as  $\lambda$ , again in the notation of Birch and Swinnerton-Dyer. Finally, according to a result of Birch and Stephens [1], one sees that  $\lambda + \lambda_1$  is even for  $D \equiv 1 \text{ or } 3 \pmod{8}$ , and odd when  $D \equiv 5 \text{ or } 7 \pmod{8}$ . Birch and Swinnerton-Dyer refer to  $\lambda + \lambda_1 - 2$  as the ‘number of first descents’, however it should be noted that this is not in general the same as our  $s(D)$ .

A completely elementary proof of the parity condition for  $s(D)$  has recently been given by Monsky. This is included as an appendix to this paper.

Our theorems lead to a number of corollaries.

**Corollary 1** *For any fixed positive integer  $r$  we have*

$$\frac{\#\{D \in S(X, h); s(D) \geq r\}}{\#S(X, h)} \leq 1.7313 \dots \times 2^{-(r^2-r)/2} + o(1)$$

as  $X \rightarrow \infty$ .

**Corollary 2** *For  $h = 1$  or  $3$  we have*

$$\sum_{D \in S(X, h)} s(D) = c' \#S(X, h) + o(X)$$

as  $X \rightarrow \infty$ , where

$$c' = \sum_{k=0}^{\infty} \frac{1}{2^k + 1} - \frac{1}{2} \prod_{k=1}^{\infty} \left( \frac{1 - 2^{-k}}{1 + 2^{-k}} \right) = 1.2039 \dots$$

Similarly, if  $h = 5$  or  $7$ , then

$$\sum_{D \in S(X, h)} s(D) = c'' \#S(X, h) + o(X)$$

as  $X \rightarrow \infty$ , where

$$c'' = \sum_{k=0}^{\infty} \frac{1}{2^k + 1} + \frac{1}{2} \prod_{k=1}^{\infty} \left( \frac{1 - 2^{-k}}{1 + 2^{-k}} \right) = 1.3250 \dots$$

Since  $r(D) \leq s(D)$  we deduce:-

**Corollary 3** For any fixed positive integer  $r$  we have

$$\frac{\#\{D \in S(X, h); r(D) \geq r\}}{\#S(X, h)} \leq 1.7313 \dots \times 2^{-(r^2 - r)/2} + o(1)$$

as  $X \rightarrow \infty$ .

**Corollary 4** For  $h = 1$  or  $3$  we have

$$\sum_{D \in S(X, h)} r(D) \leq c' \#S(X, h) + o(X)$$

as  $X \rightarrow \infty$ , and if  $h = 5$  or  $7$ , then

$$\sum_{D \in S(X, h)} r(D) \leq c'' \#S(X, h) + o(X)$$

as  $X \rightarrow \infty$ . Here  $c'$  and  $c''$  are as in Corollary 2.

Corollaries 1 and 3 show that the proportion of curves with large rank, or indeed with large Selmer rank, decreases extremely rapidly as  $D$  tends to infinity. While Theorem 2 describes the distribution of  $s(D)$  completely, the situation regarding  $r(D)$  remains in considerable doubt. In fact it seems quite probable that  $r(D)$  is only greater than 1 on a set of integers  $D$  of density zero.

Brumer and Heath-Brown [3] have investigated the proportion of large ranks as one averages over all elliptic curves. Their result is, however, subject to a number of hypotheses, and gives only an upper bound of the form

$$\ll \exp\left(-\frac{r}{20} \log(11r)\right)$$

for the ratio analogous to that of Corollary 3. Moreover, they have also considered the mean value of the rank as one averages over an arbitrary family of quadratic twists. Subject again to a number of hypotheses, it is shown that the average rank is at most 1.5. The same upper bound was obtained unconditionally for the curves (1) in the first paper [5] of this series. Corollary 4 therefore

represents an improvement on both these results. The size of the improvement is however somewhat disappointing, especially in the case in which  $s(D)$  is even, since one then expects that  $r(D) = 0$  in most cases. One is therefore led to ask whether one can get more information by considering a second descent. At present however there is little indication as to what one should expect from this.

Corollary 1 lends support to the suggestion that the maximum order of  $s(D)$  is  $O((\log D)^{1/2+\varepsilon})$ . Indeed if the bound in Theorem 1 were uniform in  $k$  one would have  $s(D) \ll (\log D)^{1/2}$ . In the reverse direction it was shown in [5; Theorem 2] that  $s(D)$  is often as large as  $(\log D)^{1/2}$ . There is no difficulty in establishing Theorem 1 with an error term in which the dependence on  $k$  is explicit. However, with the present method, the error would in fact grow very rapidly as  $k$  increases, so that no new upper bound for  $s(D)$  can in fact be obtained. It remains an interesting open problem to improve on the trivial upper bound

$$s(D) \ll \frac{\log D}{\log \log D},$$

which follows from the estimate  $s(D) \leq 2\omega(D)$ . Indeed it would be of interest to know whether the bound

$$r(D) \ll \frac{\log D}{\log \log D}$$

can be sharpened. Whereas we have a reasonable conjecture as to the maximum order of magnitude of  $s(D)$ , it is not clear whether or not  $r(D)$  is even unbounded.

We remark that there is little difficulty in extending all our results to other congruence classes  $D \equiv a \pmod{q}$  with  $q$  even and  $(a, q) = 1$ . A little thought will show that one gets exactly the same constants  $c_k$  in the corresponding version of Theorem 1. Moreover the analogue of Theorem 2 also holds with the same constants  $c'$  and  $c''$ , except when  $8 \nmid q$ , in which case the corresponding constant is merely  $(c' + c'')/2$ . The interested reader should be able to make the necessary modifications to the proofs for himself.

A more interesting question concerns the extent to which these results can be extended to other families of quadratic twists. It seems very likely that one should be able to handle the twists of any curve with three rational 2-division points, this being the condition under which the full 2-descent can be carried out without having to extend the groundfield. One would expect a parity property for the corresponding Selmer rank, similar to that given in the appendix to this paper. If one were to find an analogue of Theorem 1 in which the constants corresponding to  $c_k$  were once again independent of the parity of  $s(D)$ , then the frequencies corresponding to  $d_r$  would have to be closely related to those occurring in Theorem 2. One could indeed conjecture that the limiting frequencies given by Theorem 2 also arise in the general case. We present some numerical evidence later in this section, which suggests that one obtains the same frequencies for  $s(2D)$ , for the curve (1).

It may in fact be possible to carry through some form of analogue of our analysis for the quadratic twists of an arbitrary elliptic curve. One can only carry out the full 2-descent over the field of 2-division points, which will be a cubic number field in general. This field is fixed, and should play a relatively minor rôle. However one will then have to average over values of  $D$  lying in the field, not just over rational integers.

We remark that one can replace the  $o_k(X)$  term in Theorem 1 by

$$O_k(X(\log X)^{-1/4^k}(\log \log X)^{4^k}),$$

as is apparent from the proof. It is not clear how one might improve this, even under the assumption of, say, the Generalized Riemann Hypothesis for the relevant Dirichlet  $L$ -functions. Thus the rate of convergence to the correct asymptotic value in Theorem 1 is potentially extremely slow. Indeed the proof involves factorizing  $D$  into  $16^k$  factors. In order to average successfully over any such factor, as is necessary for the proof, each factor must be large. This is impossible unless  $D$  has at least  $16^k$  prime factors, which will usually require  $D$  to exceed  $\exp \exp(16^k)$ . It is natural to ask whether this situation is an artefact of our particular proof, or whether it genuinely reflects an extremely slow convergence to the limiting distribution. With this in mind we present the results of some numerical calculations. Rather than investigate  $s(D)$  for specific values of  $D$  we adopt a rather different procedure. If  $D$  is a product of distinct odd primes  $p_1, \dots, p_k$ , then  $s(D)$  will be determined solely by the congruence classes of the  $p_i$  modulo 8, together with the Legendre symbols  $(p_i/p_j)$  for  $i < j$ . Moreover these are independent, and as the primes vary, all possibilities will occur asymptotically equally often. When  $D$  is prime one sees that  $s(D)$  is 2 for  $D \equiv 1 \pmod{8}$ , is 0 for  $D \equiv 3 \pmod{8}$ , and is 1 for  $D \equiv 5$  or  $7 \pmod{8}$ . Similarly for  $\omega(D) = 2$  one finds that for  $D \equiv 1 \pmod{8}$  one gets the values  $s(D) = 0, 2, 4$  with frequencies 0.250, 0.625, and 0.125 respectively, while for  $D \equiv 3 \pmod{8}$  one has  $s(D) = 0, 2$  both with frequency 0.5. Such figures might reasonably lead one to expect that the limiting frequencies are heavily dependent on the congruence class of  $D$  modulo 8, and it is for precisely this reason that a congruence condition has been imposed on  $D$  throughout this paper. None the less the constant  $c_k$  which occurs in Theorem 1 is independent of  $h$ , and the limiting distributions in Theorem 2 are identical for  $h = 1$  and  $h = 3$ , as they are for  $h = 5$  and  $h = 7$ . This is really rather surprising.

One might hope to continue the calculation described above to obtain the exact frequency distribution for  $s(D)$ , for each congruence class modulo 8, for a range of values of  $\omega(D)$ . However, since there are roughly  $2^{k^2/2}$  cases to consider when  $\omega(D) = k$ , this rapidly becomes unfeasable. Thus in our calculations we consider a fixed value of  $k$  and choose the residue classes of the primes  $p_i$  modulo 8, and the values of the Legendre symbols  $(p_i/p_j)$ , at random. Following the method of Monsky's appendix to this paper, one can now compute  $s(D)$  by finding the rank of an appropriate  $2k \times 2k$  matrix, with coefficients in  $\mathbb{Z}_2$ . We

	$k = 3$	$k = 5$	$k = 10$	$k = 20$	$k = \infty$
$s(D) = 0$	0.1875	0.1785	0.1905	0.2083	0.2097
$s(D) = 1$	0.3641	0.3650	0.4004	0.4163	0.4194
$s(D) = 2$	0.2607	0.2719	0.2883	0.2841	0.2796
$s(D) = 3$	0.1220	0.1239	0.0994	0.0784	0.0799
$s(D) = 4$	0.0531	0.0441	0.0174	0.0120	0.0107
$s(D) = 5$	0.0102	0.0135	0.0033	0.0009	0.0007
$s(D) = 6$	0.0024	0.0029	0.0006	0.0000	0.0000
$s(D) = 7$	0.0000	0.0002	0.0001	0.0000	0.0000
$\sum \nu_s 2^s$	4.2641	4.3361	3.3749	3.0253	3.0000
$\sum \nu_s 4^s$	47.4919	54.1873	24.6961	15.4303	15.0000

Table 1: Estimated Frequency of Selmer Ranks for  $\omega(D) = k$

performed 10,000 random trials for each value of  $k$ . The results are summarized in the table. The table shows the frequency  $\nu_s$  of each value of  $s = s(D)$  found, together with the sums corresponding to the exponents  $k = 2$  and  $4$  in Theorem 1. The final column shows the limiting values given by Theorems 1 and 2. We remark that, for the first three rows for example, one standard deviation is roughly 0.005. The figures show that when  $\omega(D)$  is small,  $s(D)$  tends to take large values more frequently than predicted by Theorem 2. The agreement with the frequencies in Theorem 2 is reasonably good for  $k = 20$ , but for the remaining values of  $k$  it is not, particularly when  $s(D) \geq 3$ . The figures clearly illustrate the principle that one should regard the rate of convergence to the limiting distribution as depending on  $\omega(D)$ , rather than on  $D$ . With this in mind we remark that the first integer with  $\omega(D) = 20$ , is of order  $10^9$ , while the average order of  $\omega(D)$  does not reach 20 until around  $10^{10^9}$ . Thus  $D$  must be extremely large before one can expect  $s(D)$  to behave in accordance with the frequencies in the last two columns of the table.

One can do an analogous calculation for even values of  $D$ , again based on the method of Monsky's appendix. With 10,000 trials for  $k = 20$  the proportions found were 0.2110 for  $s(D) = 0$ ; 0.4173 for  $s(D) = 1$ ; 0.2759 for  $s(D) = 2$ ; 0.0818 for  $s(D) = 3$ ; 0.0130 for  $s(D) = 4$ ; and 0.0009 for  $s(D) = 5$ . These figures agree remarkably closely with the limiting frequencies for the case of odd  $D$ .

We conclude this introduction with some brief remarks about the proof. The argument is based on the earlier paper [5] of this series, which provides a convenient formula for  $2^{s(D)}$ , together with various techniques which are used to dismiss many of the contributions to the averages we shall calculate. The first new feature in the present paper is a combinatorial device, introduced in §2, which allows us to describe the indices in a crucial  $16^k$ -fold sum by means of vectors in a  $4k$ -dimensional vector space over  $\mathbb{Z}_2$ . The second major part of the paper, in §§6 and 7, is the simplification of the leading terms in the

average occurring in Theorem 1. Here again the computation is performed via linear algebra over  $\mathbb{Z}_2$ . The calculation is technically somewhat intricate, and far removed from the subject matter of our initial problem.

Finally it is a pleasure to record the help offered on the one hand by Professor Paul Monsky, who has kindly allowed his appendix to be added to this paper, and who made many helpful observations, and on the other hand by the referee, whose comments on an earlier version of this paper encouraged the author to improve the results therein considerably.

## 2 A Formula for $2^{ks(D)}$ .

In this section we shall use results from our previous work [5] to write down an expression for  $2^{ks(D)}$ . Our starting point is Lemma 3 of [5], which we restate here for convenience.

**Lemma 1** *We have*

$$2^{s(D)} = \sum_{\mathbf{D}} g(\mathbf{D}), \quad (2)$$

where the sum is taken over all factorizations

$$D = \prod_{i,j} D_{ij}, \quad 1 \leq i \leq 4, \quad 0 \leq j \leq 4, \quad j \neq i,$$

and where

$$g(\mathbf{D}) = \left(\frac{-1}{\alpha}\right) \left(\frac{2}{\beta}\right) \prod_i 4^{-\omega(D_{i0})} \prod_{j \neq 0} 4^{-\omega(D_{ij})} \prod_{k \neq i,j} \prod_l \left(\frac{D_{kl}}{D_{ij}}\right)$$

with

$$\alpha = D_{12}D_{14}D_{23}D_{21}, \quad \beta = D_{24}D_{21}D_{34}D_{31}.$$

In order to clarify the combinatorics of the situation a better system of notation will be required. We therefore index the various factors of  $D$  by means of elements of  $\mathbb{Z}_2^4$ , according to the following table.

$$\begin{array}{llll} D_{10} = D_{0001}, & D_{12} = D_{1011}, & D_{13} = D_{1001}, & D_{14} = D_{0011}, \\ D_{20} = D_{0100}, & D_{21} = D_{1110}, & D_{23} = D_{0110}, & D_{24} = D_{1100}, \\ D_{30} = D_{0101}, & D_{31} = D_{1101}, & D_{32} = D_{0111}, & D_{34} = D_{1111}, \\ D_{40} = D_{0000}, & D_{41} = D_{0010}, & D_{42} = D_{1000}, & D_{34} = D_{1010}. \end{array}$$

By abuse of notation we shall simply refer to ‘the variable  $u$ ’, say, where  $u \in \mathbb{Z}_2^4$ . One can then check, by a somewhat tedious calculation, that the Jacobi symbol

$$\left(\frac{D_u}{D_v}\right)$$



occurs in the expression for  $2^{s(D)}$  precisely when  $B(u, v) = 1$ , where  $B$  is the polynomial

$$B(u, v) = v_1(u_4 + v_4) + v_3(u_2 + v_2).$$

We now recall that, according to §3 of [5], two variables  $D_{ij}$  and  $D_{kl}$ , in the old notation, are said to be ‘linked’ if  $i \neq k$ , and precisely one of the conditions  $l \neq 0, i$  or  $j \neq 0, k$ , holds. As remarked in [2], this means that exactly one of the Jacobi symbols

$$\left(\frac{D_{kl}}{D_{ij}}\right), \quad \left(\frac{D_{ij}}{D_{kl}}\right)$$

occurs in the expression for  $g(\mathbf{D})$ . If  $P$  is the quadratic form

$$P(w_1, w_2, w_3, w_4) = w_1w_4 + w_2w_3$$

we have  $B(u, v) + B(v, u) = P(u + v)$ , and so it follows that, in the new notation, the variables  $u$  and  $v$  are linked exactly when  $P(u + v) = 1$ . Moreover it is apparent that the variable  $u$  is a factor of  $\alpha$  in Lemma 1 exactly when  $Q(u) = 1$ , where  $Q$  is the quadratic form

$$Q(w_1, w_2, w_3, w_4) = w_2w_3 + w_3w_4.$$

Similarly  $u$  is a factor of  $\beta$  when  $R(u) = 1$ , where  $R$  is the quadratic form

$$R(w_1, w_2, w_3, w_4) = w_1w_2.$$

We can therefore recast (2) as

$$2^{s(D)} = \sum_{\prod D_u = D} \left( \prod_u 4^{-\omega(D_u)} \left(\frac{-1}{D_u}\right)^{Q(u)} \left(\frac{2}{D_u}\right)^{R(u)} \right) \left( \prod_{u,v} \left(\frac{D_u}{D_v}\right)^{B(u,v)} \right).$$

We are now ready to consider the  $k$ -th power of the above expression. This will give us a sum in which  $D$  has  $k$  potentially different factorisations into 16 divisors,

$$D = \prod_{u \in \mathbb{Z}_2^4} D_u^{(j)} \quad 1 \leq j \leq k.$$

We may specify these factorisations by giving each of the highest common factors

$$\text{h.c.f.}(D_{u^{(1)}}, \dots, D_{u^{(k)}}) = D_{u^{(1)} \dots u^{(k)}},$$

say, where  $u^{(1)}, \dots, u^{(k)}$  run independently over  $\mathbb{Z}_2^4$ . We therefore obtain a system of  $16^k$  divisors  $D_v$ , indexed by  $v \in \mathbb{Z}_2^{4k}$ , whose product is  $D$ .

The product

$$\prod_{j=1}^k \prod_{u^{(j)}} \left(\frac{-1}{D_{u^{(j)}}}\right)^{Q(u^{(j)})}$$

now becomes

$$\prod_v \left(\frac{-1}{D_v}\right)^{Q(v)},$$

where, for a vector

$$v = u^{(1)} \dots u^{(k)} \in \mathbb{Z}_2^{4k},$$

we have defined

$$Q(v) = \sum_j Q(u^{(j)}).$$

The other factors behave analogously, and we therefore conclude as follows.

**Lemma 2** *We have*

$$2^{ks(D)} = \sum_{\mathbf{D}} g_k(\mathbf{D}),$$

where  $\mathbf{D}$  runs over sets

$$\mathbf{D} = \{D_v; v \in \mathbb{Z}_2^{4k}, \prod_v D_v = D\},$$

and

$$g_k(\mathbf{D}) = \left( \prod_u 4^{-k\omega(D_u)} \left(\frac{-1}{D_u}\right)^{Q(u)} \left(\frac{2}{D_u}\right)^{R(u)} \right) \left( \prod_{u,v} \left(\frac{D_u}{D_v}\right)^{B(u,v)} \right).$$

Here

$$Q(v) = \sum_{j=0}^{k-1} (v_{4j+2}v_{4j+3} + v_{4j+3}v_{4j+4}),$$

$$R(v) = \sum_{j=0}^{k-1} v_{4j+1}v_{4j+2},$$

and

$$B(u, v) = \sum_{j=0}^{k-1} \{v_{4j+1}(u_{4j+4} + v_{4j+4}) + v_{4j+3}(u_{4j+2} + v_{4j+2})\}.$$

### 3 Averaging Over $D$

In this section we begin our estimation of

$$\sum_{D \in S(X, h)} 2^{ks(D)}.$$

Instead of summing over  $D$  we sum over the  $16^k$  variables  $D_u$ , subject to the conditions that each  $D_u$  is square-free, that they are coprime in pairs, and that their product  $D$  satisfies

$$D \leq X, \quad D \equiv h \pmod{8}.$$

We divide the range of each variable  $D_u$  into intervals  $(A_u, 2A_u]$  where  $A_u$  runs over powers of 2. Notice that there will be an interval  $(\frac{1}{2}, 1]$  containing only the integer 1, corresponding to  $A_u = 2^{-1}$ . This subdivision will give us

$$O(\log^{16^k} X)$$

non-empty subsums, which we shall write as  $S(\mathbf{A})$ , where  $\mathbf{A}$  is the  $16^k$ -tuple of numbers  $A_u$ . Here we may suppose that

$$1 \ll \prod A_u \ll X. \quad (3)$$

We begin by eliminating those sums  $S(\mathbf{A})$  for which at most  $4^k - 1$  of the  $A_u$  are 'large'. Specifically let

$$B = (\log X)^{33.16^k},$$

Then if  $\sum'$  indicates the condition that at most  $4^k - 1$  of the  $A_u$  satisfy  $A_u \geq B$  we have

$$\sum_{A_u}' |S(\mathbf{A})| \leq \sum_{\prod D_u \leq X} \prod_u 4^{-k\omega(D_u)},$$

where the  $D_u$  are square-free and coprime in pairs, and at most  $4^k - 1$  of the  $D_u$  have  $D_u \geq 2B$ . We write

$$m = \prod_{D_u < 2B} D_u, \quad n = \prod_{D_u \geq 2B} D_u,$$

so that  $m \leq (2B)^{16^k}$  and  $n \leq X/m$ . Now a square-free integer  $g$ , say, can be written as a product of  $r$  or fewer factors in

$$1 + d(g) + d_3(g) + \dots + d_r(g) \leq r d_r(g) = r^{1+\omega(g)}$$

ways. We therefore see that each value of  $m$  can arise at most  $16^{k(1+\omega(m))}$  times, and each value of  $n$  can arise at most

$$\{4^k - 1\}^{1+\omega(n)}$$

times. We may now deduce that

$$\sum_{A_u}' |S(\mathbf{A})| \ll \sum_m 4^{k\omega(m)} \sum_n (1 - 4^{-k})^{\omega(n)}.$$

We now use the bound

$$\sum_{n \leq N} \gamma^{\omega(n)} \ll N(\log N)^{\gamma-1}, \quad (4)$$

which is valid for any fixed  $\gamma > 0$ . Since

$$X/m \gg XB^{-16^k} \gg X^{1/2},$$

we have  $\log X/m \gg \log X$ , and we therefore find that

$$\sum_{A_u} |S(\mathbf{A})| \ll X(\log X)^{-1/4^k} \sum_m 4^{k\omega(m)} m^{-1}.$$

A second application of (4), together with partial summation, shows that

$$\sum_{m \leq M} 4^{k\omega(m)} m^{-1} \ll \log^{4^k} M,$$

whence

$$\sum_{A_{ij}} |S(\mathbf{A})| \ll X(\log X)^{-1/4^k} \log^{4^k} M \ll X(\log X)^{-1/4^k} (\log \log X)^{4^k}.$$

We consider next the sums  $S(\mathbf{A})$  for which there are linked indices  $u, v$  for which  $A_u, A_v$  are both large. As in [5] we use the following lemma, whose proof may be found in [5;§6].

**Lemma 3** *Let  $a_m, b_n$  be complex numbers of modulus at most 1. Let an odd number  $h$  be given and let  $M, N, X \gg 1$ . Then*

$$\sum_{m,n} \left(\frac{n}{m}\right) a_m b_n \ll MN \{\min(M, N)\}^{-1/32},$$

*uniformly in  $X$ , where the sum is for square-free  $m, n$  satisfying  $M < m \leq 2M$ ,  $N < n \leq 2N$ ,  $mn \leq X$ , and  $mn \equiv h \pmod{8}$ .*

Now, if  $u$  and  $v$  are linked we can write  $g_k(\mathbf{D})$  in the form

$$g_k(\mathbf{D}) = \left(\frac{D_u}{D_v}\right) a(D_u) b(D_v),$$

where the function  $a(D_u)$  depends on all the other variables  $D_w$ , say, as well as  $D_u$ , but is independent of  $D_v$ , and similarly for the function  $b(D_v)$ . Moreover we have

$$|a(D_u)|, |b(D_v)| \leq 1.$$

We can now write

$$|S(\mathbf{A})| \leq \sum_{D_w} \left| \sum_{D_u, D_v} \left( \frac{D_u}{D_v} \right) a(D_u) b(D_v) \right|.$$

The conditions that  $D_u$  and  $D_v$  should be coprime to each of the  $D_w$  may be expressed by taking the functions  $a$  and  $b$  to vanish at appropriate values. Moreover the Jacobi symbol is automatically zero if the  $D_u$  and  $D_v$  are not coprime. The remaining conditions on these two variables may therefore be expressed by insisting that they are square-free and satisfy

$$D_u D_v \equiv h' \pmod{8}, \quad D_u D_v \leq X',$$

where  $h'$  and  $X'$  will depend on the other variables  $D_w$ . It now follows from Lemma 3 that if  $A_u, A_v \geq B$  then

$$S(\mathbf{A}) \ll \left( \prod_w A_w \right) A_u A_v \{ \min(A_u, A_v) \}^{-1/32} \ll X B^{-1/32},$$

by (3). We therefore deduce as follows.

**Lemma 4** *We have*

$$S(\mathbf{A}) \ll X B^{-1/32}$$

*whenever there is a pair of linked indices with*

$$A_u, A_v \geq B.$$

Now let

$$C = \exp\{\kappa(\log \log X)^2\},$$

where  $\kappa > 0$  is a constant to be specified in due course. We proceed to examine the case in which  $A_u \geq C$ , but every index  $v$  to which  $u$  is linked has  $A_v < B$ . We write  $D'$  for the product of the corresponding variables  $D_v$ . Using the law of quadratic reciprocity we can now put  $g(\mathbf{D})$  into the shape

$$4^{-k\omega(D_u)} \left( \frac{D_u}{D'} \right) \chi(D_u) c,$$

where  $\chi$  is a character modulo 8, which may depend on the variables  $D_v$  other than  $D_u$ , and where the remaining factor  $c$  is independent of  $D_u$  and satisfies  $|c| \leq 1$ . It follows that

$$|S(\mathbf{A})| \leq \sum_{D_v} \left| \sum_{D_u} 4^{-k\omega(D_u)} \left( \frac{D_u}{D'} \right) \chi(D_u) \right|, \quad (5)$$

where the inner sum is restricted by the conditions that  $D_u$  must be square-free and coprime to all the other variables  $D_v$ , and that

$$D_u \equiv h' \pmod{8}, \quad A_u < D_u \leq \min(2A_u, X'),$$

where  $h'$  and  $X'$  depend on the variables  $D_v$  other than  $D_u$ . We now apply the following result, which is a trivial modification of [5; Lemma 6]. The reader is referred to [5; §6] for the proof.

**Lemma 5** *Let  $N > 0$  be given. Then for arbitrary positive integers  $q, r$  and any non-principal character  $\chi \pmod{q}$ , we have*

$$\sum_{n \leq x, (n, r)=1} \mu^2(n) 4^{-k\omega(n)} \chi(n) \ll xd(r) \exp(-c\sqrt{\log x})$$

with a positive constant  $c = c_N$ , uniformly for  $q \leq \log^N x$ .

To use this result we remove the condition  $D_u \equiv h' \pmod{8}$  from the inner sum on the right of (5) and insert instead a factor

$$\frac{1}{4} \sum_{\psi \pmod{8}} \psi(D_u) \overline{\psi(h')}.$$

Taking

$$q = 8D' \ll B^{16^k} \ll (\log X)^N$$

with  $N = 33.16^{2k}$  and  $r = \prod D_v$ , we conclude that

$$S(\mathbf{A}) \ll A_u \exp(-c\sqrt{\log A_u}) \sum_{D_v} d(r),$$

providing that  $D' \neq 1$ . Since the variables  $D_v$  are coprime in pairs we have  $d(r) = \prod d(D_v)$ . Moreover for a single variable  $D_v$  we will have

$$\sum_{D_v} d(D_v) \ll A_v \log A_v \ll A_v \log X,$$

whence (3) yields

$$S(\mathbf{A}) \ll X(\log X)^{16^k} \exp(-c\sqrt{\log A_u}) \ll X(\log X)^{16^k - c\sqrt{\kappa}},$$

providing that  $D' \neq 1$  and  $A_u \geq C$ . Bearing in mind that there are  $O(\log^{16^k} X)$  sums  $S(\mathbf{A})$  we require that

$$\sqrt{\kappa} > c^{-1} 2.16^k.$$

In view of Lemma 4 we can now conclude as follows.

**Lemma 6** *We have*

$$\sum_{\mathbf{A}} |S(\mathbf{A})| = o_k(X),$$

where the sum over  $\mathbf{A}$  is for all sets in which either there are at most  $4^k - 1$  elements  $A_u \geq C$ , or there are linked indices  $u$  and  $v$  with  $A_u \geq C$  and  $A_v \geq 1$ .

## 4 Linked Indices

Those subsums not handled by Lemma 6 have at least  $4^k$  ‘large’ variables  $D_u$ , no two of which are linked. The situation is described more precisely in the next lemma.

**Lemma 7** *Let  $\mathcal{U} \subseteq \mathbb{Z}_2^{4k}$  be a collection of unlinked indices. Then  $\#\mathcal{U} \leq 4^k$ , and if  $\#\mathcal{U} = 4^k$  then  $\mathcal{U}$  is either a vector subspace of  $\mathbb{Z}_2^{4k}$  or a coset of such a subspace.*

It clearly suffices to prove the lemma under the assumption that  $\mathcal{U}$  is a maximal collection of unlinked indices. According to the description in §2, we have  $P(u + v) = 0$  for  $u, v \in \mathcal{U}$ . Thus if  $\mathcal{U}$  is a maximal unlinked set, so is any translate  $\mathcal{U} + u$ . We may therefore assume, with no loss of generality, that  $\mathcal{U}$  contains the vector 0. We now claim that, under this condition,  $\mathcal{U}$  will be closed under addition. For if  $0, u, v, w \in \mathcal{U}$ , then

$$P(u + v) = P(u + w) = P(v + w) = P(u + 0) = P(v + 0) = P(w + 0) = 0,$$

since any two elements of  $\mathcal{U}$  are unlinked. It follows that the indices  $u + v$  and  $w$  are unlinked, since

$$P((u + v) + w) = P(u + v) + P(u + w) + P(v + w) + P(u) + P(v) + P(w) = 0.$$

If we now allow  $w$  to vary over  $\mathcal{U}$  we see that  $\mathcal{U} \cup \{u + v\}$  must be an unlinked set. The maximality of  $\mathcal{U}$  therefore implies that  $u + v \in \mathcal{U}$  as required.

It remains to ask which subspaces  $\mathcal{U}$  of  $\mathbb{Z}_2^{4k}$  are isotropic for  $P$ . This question is answered by the following lemma, which shows that a subspace which is unlinked can have dimension at most  $2k$ . This, of course suffices for the proof of Lemma 7.

**Lemma 8** *Let  $V$  be a vector space over  $\mathbb{Z}_2$ , of dimension  $2n$ . If  $F$  is a quadratic form on  $V$  we write  $F(u, v) = F(u + v) - F(u) - F(v)$ , so that  $F$  is a symmetric bilinear form on  $V$ , and we say that  $F$  is non-singular if  $F(u, v) = 0$  for all  $v \in V$  implies  $u = 0$ . Then if  $F$  is non-singular and there is a vector  $c \in V$  such that  $F(u + c) = F(c)$  for all  $u$  in some subspace  $U$  of  $V$ , we have  $\dim(U) \leq n$ .*

We begin by observing that the condition  $F(u + c) = F(c)$  may be rewritten as  $F(u) + F(u, c) = 0$ . If we choose a basis and write  $u = (u_1, \dots, u_{2n})$  then, for appropriate  $\lambda_i \in \mathbb{Z}_2$ , we have

$$F(u, c) = \sum_{i=1}^{2n} \lambda_i u_i = \sum_{i=1}^{2n} \lambda_i u_i^2,$$

since  $u_i \in \mathbb{Z}_2$ . The condition  $F(u + c) = F(c)$  then becomes  $F_c(u) = 0$ , where the quadratic form  $F_c$  is given by

$$F_c(u) = F(u) + \sum_{i=1}^{2n} \lambda_i u_i^2. \quad (6)$$

Notice that  $F_c$  induces the same bilinear form  $F(u, v)$  as  $F$  does. Since  $F$  is non-singular, the map

$$v \rightarrow F(v, *)$$

gives an isomorphism between  $V$  and its dual. The condition  $F_c(u) = 0$  yields

$$F(u_1, u_2) = F_c(u_1 + u_2) - F_c(u_1) - F_c(u_2) = 0$$

for all  $u_1, u_2 \in U$ . The above isomorphism therefore embeds  $U$  in its annihilator. We deduce that  $\dim(U) \leq 2n - \dim(U)$ , and the lemma immediately follows.

We end this section with some further results of the same general type, which will be useful later.

**Lemma 9** *Let  $V$  be as above, and let  $F$  be a non-singular quadratic form on  $V$ . Suppose that  $F(u) = 0$  for all  $u$  in some  $n$ -dimensional subspace  $U$  of  $V$ . Then there are  $2^{2n-1} + 2^{n-1}$  vectors  $v \in V$  for which  $F(v) = 0$ .*

To prove this we take any direct complement,  $W$ , say, of  $U$  and observe that the map

$$v \rightarrow F(v, *) \tag{7}$$

takes  $V$  to the dual of  $U$ . If  $w \in W$  corresponds to the zero functional, then  $w$  is in the inverse image of the annihilator  $U^\circ$ . As in the proof of Lemma 8 this inverse image is  $U$  itself. It follows that  $w = 0$  since  $U \cap W = \{0\}$ . It follows that (7) produces a non-zero functional for all  $w \in W \setminus \{0\}$ . Now  $F(u + w) = 0$  requires  $F(w, u) = F(w)$ , which will have  $2^{n-1}$  solutions  $u$  for every  $w$  for which (7) is non-zero, and  $2^n$  solutions  $u$  when  $w = 0$ . The total number of solutions is therefore

$$(2^n - 1)2^{n-1} + 2^n = 2^{2n-1} + 2^{n-1},$$

as required.

**Lemma 10** *Let  $V$  be as above, and let  $F$  be a non-singular quadratic form on  $V$ . Suppose that  $F(u) = 0$  for all  $u$  in some  $n$ -dimensional subspace  $U$  of  $V$ , and suppose there exists a vector  $c \in V$  and a second subspace  $W \subseteq V$ , also of dimension  $n$ , such that  $F(w + c) = F(c)$  for all  $w \in W$ . Then  $F(c) = 0$ .*

We construct  $F_c$  as in the proof of Lemma 8, and deduce from Lemma 9 that  $F_c(v) = 0$  has  $2^{2n-1} + 2^{n-1}$  solutions. It follows that  $F(v + c) = F(c)$  also has  $2^{2n-1} + 2^{n-1}$  solutions, and hence also that  $F(v) = F(c)$  does, since  $v + c$  runs over all of  $V$ . If  $F(c) = 1$  then we deduce that  $F(v) = 0$  has only  $2^{2n-1} - 2^{n-1}$  solutions. In view of our assumption concerning the subspace  $U$ , this would contradict Lemma 9. Hence  $F(c)$  must equal zero, as required.

**Lemma 11** *Define the quadratic form  $P^{(n)}$  on  $\mathbb{Z}_2^{2n}$  by*

$$P^{(n)}(x_1, \dots, x_{2n}) = \sum_{h=1}^n x_{2h-1} x_{2h}. \tag{8}$$



Then there are exactly

$$\prod_{j=1}^n (2^{j-1} + 1)$$

$n$ -dimensional subspaces  $U$  of  $\mathbb{Z}_2^{2n}$  on which  $P^{(n)}$  vanishes.

We shall write  $P^{(n)} = P$  for brevity for most of the proof. We write  $G_n$  for the number of subspaces of the type required, and we observe that  $G_1 = 2$ . This will form the base step of an induction argument. Each space  $U$  contains  $2^n - 1$  non-zero vectors  $v$ , each of which must lie on the quadric  $P = 0$ . It follows that

$$(2^n - 1)G_n = \sum_{P(v)=0, v \neq 0} \#\{U : P|_U = 0, \dim(U) = n, v \in U\}. \quad (9)$$

To handle the right hand side of (9) we first observe that if  $v$  is any non zero vector on  $P = 0$  then we can choose a basis  $v = v_1, v_2, \dots, v_{2n}$  for  $\mathbb{Z}_2^{2n}$  which puts  $P$  again into the form (8). To do this let  $v = (x_1, \dots, x_{2n})$ , where we may suppose, without loss of generality, that  $x_1 = 1$ . If  $e_1, \dots, e_{2n}$  is the old coordinate basis we then take  $v_2 = e_2$  and

$$v_{2h-1} = e_{2h-1} + x_{2h}e_2, \quad v_{2h} = e_{2h} + x_{2h-1}e_2, \quad 2 \leq h \leq n.$$

We therefore see that

$$\#\{U : P|_U = 0, \dim(U) = n, v \in U\}$$

is independent of  $v$ , so that (9) yields

$$\begin{aligned} G_n &= \frac{\#\{v \neq 0 : P(v) = 0\}}{2^n - 1} \#\{U : P|_U = 0, \dim(U) = n, e_1 \in U\} \\ &= \frac{2^{2n-1} + 2^{n-1} - 1}{2^n - 1} \#\{U : P|_U = 0, \dim(U) = n, e_1 \in U\} \\ &= (2^{n-1} + 1) \#\{U : P|_U = 0, \dim(U) = n, e_1 \in U\} \end{aligned}$$

by Lemma 9. Finally we see that if  $e_1 \in U$  then the  $e_2$  component of every vector in  $U$  must vanish. There is therefore a one to one correspondence between subspaces  $U$  of the type considered above and subspaces

$$U^* \leq \mathbb{Z}_2^{2n-2}, \quad P^{(n-1)}|_{U^*} = 0, \quad \dim(U^*) = n - 1,$$

given by omitting the first two coordinates of every vector in  $U$ . Hence

$$\#\{U : P|_U = 0, \dim(U) = n, e_1 \in U\} = G_{n-1},$$

and the lemma follows by induction.

## 5 The Leading Terms

In view of Lemma 7 those sums  $S(\mathbf{A})$  not handled by Lemma 6 will have exactly  $4^k$  indices for which  $A_u \geq C$ , these forming an unlinked set  $\mathcal{U}$ , while all other indices have  $A_u = \frac{1}{2}$ . We shall say that such an  $\mathbf{A}$  is ‘admissible’ for  $\mathcal{U}$ . Lemma 7 shows that a set  $\mathbf{A}$  can be admissible for at most one  $\mathcal{U}$ . We now decompose the sum over  $\mathbf{D}$  according to the residue classes modulo 4 and 8 in which the various  $D_u$  lie. We shall let  $h_u$  take all possible values from the set  $\{1, 3, 5, 7\}$  as  $u$  runs over  $\mathcal{U}$ , subject to the condition that

$$\prod h_u \equiv h \pmod{8},$$

and we shall write

$$\sigma(h_u) = \left( \prod_{u \in \mathcal{U}} \left( \frac{-1}{h_u} \right)^{Q(u)} \left( \frac{2}{h_u} \right)^{R(u)} \right) \left( \prod_{u, v \in \mathcal{U}} (-1)^{B(u, v)(h_u - 1)(h_v - 1)/4} \right),$$

where the second product is over unordered pairs  $u, v$ . Then

$$S(\mathbf{A}) = \sum_{h_u} \sigma(h_u) \sum_{D_u \equiv h_u \pmod{8}} \prod_u 4^{-k\omega(D_u)}, \quad (10)$$

where  $D_u$  runs over square-free values in  $(A_u, 2A_u]$  such that  $\prod D_u \equiv h \pmod{8}$ , with the values of  $D_u$  coprime in pairs.

We may pick out the conditions  $D_u \equiv h_u \pmod{8}$  by introducing a factor

$$4^{-4^k} \prod_{u \in \mathcal{U}} \left( 1 + \left( \frac{-1}{h_u} \right) \left( \frac{-1}{D_u} \right) \right) \left( 1 + \left( \frac{2}{h_u} \right) \left( \frac{2}{D_u} \right) \right).$$

When this is expanded we will get a linear combination of terms  $\prod_u \chi_u(D_u)$ , say, where the characters  $\chi_u$  are all to modulus 8. When the characters are all the same, equal to  $\chi$ , say, the coefficient is

$$4^{-4^k} \prod_u \chi(h_u) = 4^{-4^k} \chi(h).$$

The total contribution to the inner sum on the right of (10) from the four possible characters  $\chi$  is therefore

$$4^{1-4^k} \sum_{D_u} \prod_u 4^{-k\omega(D_u)}.$$

In the remaining case let us suppose that  $\chi_u \neq \chi_v$ . We then get a contribution

$$\ll \sum_{D'} \left| \sum_{D_u, D_v} 4^{-k\omega(D_u) - k\omega(D_v)} \chi_1(D_u) \chi_2(D_v) \right|, \quad (11)$$

where  $D'$  is the product of all variables  $D_w$  other than  $D_u$  and  $D_v$ . We now call on the following result which is a trivial modification of Lemma 10 of [5].

**Lemma 12** *Let  $X > 0$  and  $M, N \geq C > 0$  be given. Then for an arbitrary positive integer  $r$ , any odd integer  $h$ , and any distinct characters  $\chi_1, \chi_2 \pmod{8}$ , we have*

$$\sum_{m,n} \mu^2(m) \mu^2(n) 4^{-k\omega(m)-k\omega(n)} \chi_1(m) \chi_2(n) \ll d(r) X \exp(-c' \sqrt{\log C}) \log X,$$

for some positive absolute constant  $c'$ , where the sum is over coprime variables satisfying the conditions

$$M < m \leq 2M, \quad N < n \leq 2N, \quad mn \leq X, \quad mn \equiv h \pmod{8}, \quad (mn, r) = 1.$$

The expression (11) is therefore

$$\begin{aligned} &\ll \sum_{D'} A_u A_v \exp(-c' \sqrt{\log C}) \log X \\ &\ll \left( \prod_{w \neq u, v} A_w \right) A_u A_v \exp(-c' \sqrt{\log C}) \log X \\ &\ll X \exp(-c' \sqrt{\log C}) \log X. \end{aligned}$$

This will make a negligible contribution to  $S(\mathbf{A})$  if the constant  $\kappa$  in the definition of  $C$  is chosen sufficiently large. We conclude that

$$S(\mathbf{A}) = 4^{1-4^k} \sum_{h_u} \sigma(h_u) \sum_{D_u} 4^{-k\omega(D)} + O(X \exp(-c' \sqrt{\log C}) \log X).$$

We proceed to sum  $S(\mathbf{A})$  over those sets  $\mathbf{A}$  which are admissible for  $\mathcal{U}$ . This will give us

$$4^{1-4^k} \sum_{h_u} \sigma(h_u) \sum_{D_u} 4^{-k\omega(D)} + O(X \exp(-c' \sqrt{\log C}) (\log X)^{1+16^k}),$$

where the sum is restricted by the conditions

$$D_u > A^*, \quad D \leq X, \quad D \equiv h \pmod{8}, \quad D \text{ square-free},$$

and  $A^*$  is the power of 2 specified by the inequalities

$$C \leq A^* < 2C.$$

We now wish to remove the condition  $D_u > A^*$ , and we can do this with the help of the estimate (4). On putting  $d = D_u$  we see that the error involved is

$$\ll \sum_{d \leq A^*} \sum_{D \leq X, d|D} \mu^2(D) 4^{-k\omega(D)} (4^k - 1)^{\omega(D/d)},$$

since  $D/d$  can be written in  $(4^k - 1)^{\omega(D/d)}$  ways as a product of the  $D_v$  for  $v \in \mathcal{U} - \{u\}$ . We therefore have an error

$$\begin{aligned} &\ll \sum_{d \leq A^*} 4^{-k\omega(d)} \sum_{e \leq X/d} (1 - 4^{-k})^{\omega(e)} \\ &\ll X(\log X)^{-4^{-k}} \sum_{d \leq A^*} 4^{-k\omega(d)} d^{-1} \\ &\ll X(\log X)^{-4^{-k}} (\log \log X)^2. \end{aligned}$$

Since  $D$  has  $4^{k\omega(D)}$  representations as a product of  $D_u$  with  $u \in \mathcal{U}$ , we see that the main term is now merely

$$\sum_{D_u} 4^{-k\omega(D)} = \sum_D 1 = S(X, h).$$

Finally we can sum over the various sets  $\mathcal{U}$ , to get

$$\begin{aligned} &\sum_{D \in S(X, h)} 2^{ks(D)} \\ &= 4^{1-4^k} \left( \sum_{\mathcal{U}} \sum_{h_u} \sigma(h_u) \right) S(X, h) + o(X) \\ &\quad + O(X \exp(-c' \sqrt{\log C}) (\log X)^{1+16^k}) + O(X(\log X)^{-4^{-k}} (\log \log X)^2). \end{aligned}$$

If the constant  $\kappa$  in the definition of  $C$  is chosen sufficiently large the above error terms will be satisfactory. This proves Theorem 1, with  $c_k$  replaced by the constant

$$4^{1-4^k} \sum_{\mathcal{U}} \sum_{h_u} \sigma(h_u) = c_{k,h},$$

say.

There remains the task of evaluating this expression. It will turn out that  $c_{k,h}$  is independent of  $h$ . However at this stage we content ourselves with one small observation. Let  $\{h_u\}$  be an admissible set of values, so that

$$\prod h_u \equiv h \pmod{8},$$

and let  $j_u$  run over values 0 or 1, subject to the condition that  $\sum j_u$  is even. Then

$$\prod (h_u + 4j_u) \equiv \prod h_u \equiv h \pmod{8},$$

so that  $\{h_u + 4j_u\}$ , taken modulo 8, is also admissible. Moreover

$$\left( \frac{2}{h_u + 4j_u} \right) = (-1)^{j_u} \left( \frac{2}{h_u} \right).$$

It follows that

$$\sum_{h_u} \sigma(h_u) = \sum_{h_u} \sigma(h_u + 4j_u) = \prod_u (-1)^{j_u R(u)} \sum_{h_u} \sigma(h_u),$$

for any set of values of  $j_u$  with  $\sum j_u$  even. We therefore see that

$$\sum_{h_u} \sigma(h_u) = 0$$

unless  $R(u)$  is constant on  $\mathcal{U}$ , in which case we shall write  $R(\mathcal{U})$  for the common value. If we now restrict  $\mathcal{U}$  to run over unlinked sets on which  $R$  is constant, and restrict  $h_u$  to take values 1 and 3 only, subject to the condition

$$\prod h_u \equiv h \pmod{4},$$

we arrive at the formula

$$c_{k,h} = 2^{1-4^k} \sum_{\mathcal{U}} \left(\frac{2}{h}\right)^{R(\mathcal{U})} \sum_{h_u} \rho(h_u), \quad (12)$$

where

$$\rho(h_u) = \left( \prod_{u \in \mathcal{U}} \left(\frac{-1}{h_u}\right)^{Q(u)} \right) \left( \prod_{u,v \in \mathcal{U}} (-1)^{B(u,v)(h_u-1)(h_v-1)/4} \right).$$

## 6 Computation of $c_{k,h}$ —‘Good’ subspaces

We write (12) in the form

$$c_{k,h} = 2^{1-4^k} \sum_{\mathcal{U}} \left(\frac{2}{h}\right)^{R(\mathcal{U})} \Sigma_{\mathcal{U}},$$

where

$$\Sigma_{\mathcal{U}} = \sum_{h_u} \rho(h_u).$$

In this section we shall show that  $\Sigma_{\mathcal{U}} = 0$  unless  $\mathcal{U}$  is a coset  $c + \mathcal{U}_0$  of a (suitably defined) ‘good’ subspace  $\mathcal{U}_0$ . We shall also show that if  $\mathcal{U}_0$  is good, then the expression for  $\Sigma_{\mathcal{U}}$  can be considerably simplified.

We begin the computation of  $c_{k,h}$  by transforming (12) so that the sum over the various choices of  $h_u$  is replaced by a sum over subsets of  $\mathcal{U}$ . It will be convenient to write  $s$  for the cardinality of  $S \subseteq \mathcal{U}$ , and similarly  $t$  for the cardinality of  $T \subseteq \mathcal{U}$ . We begin by letting  $S$  be the subset of  $\mathcal{U}$  on which  $h_u = 3$ ,

so that  $S$  runs over all subsets for which  $s \equiv h_0 \pmod{2}$ . Here  $h_0 = 1$  for  $h \equiv 3 \pmod{4}$ , and  $h_0 = 0$  otherwise. We now see that  $\rho(h_u)$  becomes  $(-1)^{e(S)}$ , where

$$e(S) = \sum_{u \in S} Q(u) + \sum_{u, v \in S} B(u, v).$$

Here  $u, v$  runs over unordered pairs as before.

For the purpose of the proof it will be convenient to interpret  $s$  and  $t$  as lying in  $\mathbb{Z}_2$ . Moreover we shall interpret the expression  $(-1)^\alpha$ , where  $\alpha \in \mathbb{Z}_2$ , in the obvious way. An important rôle in our treatment of  $c_{k,h}$  will be played by the group structure on the power set of  $\mathcal{U}$ , under the symmetric difference operator  $\triangle$ . Thus our first task is to compute  $e(S \triangle T)$ . We shall not assume here that there is a parity condition on  $s$  or  $t$ . We write

$$(-1)^{e(S)}(-1)^{e(T)} = (-1)^{e(S \triangle T)}(-1)^{e(S, T)}$$

and seek to determine  $e(S, T)$ . Since

$$\sum_{u \in S} Q(u) + \sum_{u \in T} Q(u) = \sum_{u \in S \triangle T} Q(u) + 2 \sum_{u \in S \cap T} Q(u) = \sum_{u \in S \triangle T} Q(u),$$

we see that the terms involving the function  $Q$  make no contribution to  $e(S, T)$ . To handle the terms involving  $B(u, v)$  it is convenient, just for the moment, to impose a linear ordering ' $<$ ' on the vectors in  $\mathcal{U}$ , so that we can sum over unordered pairs  $u, v$  by requiring that  $u < v$ . Then, writing

$$\Sigma(X, Y) = \sum_{u \in X, v \in Y, u < v} B(u, v),$$

we have

$$\begin{aligned} \Sigma(S, S) + \Sigma(T, T) &= \Sigma(S \triangle T, S \triangle T) + \Sigma(S, T) + \Sigma(T, S) \\ &\quad - 2\Sigma(S \setminus T, T \setminus S) - 2\Sigma(T \setminus S, S \setminus T). \end{aligned}$$

It follows that

$$e(S, T) = \Sigma(S, T) + \Sigma(T, S).$$

Since

$$B(u, v) + B(v, u) = P(u + v) = 0 \tag{13}$$

for  $u, v \in \mathcal{U}$ , we deduce that

$$\Sigma(S, T) + \Sigma(T, S) = \sum_{(u, v): u \in S, v \in T, u \neq v} B(u, v).$$

Of course  $B(u, u) = 0$ , by definition, so the condition  $u \neq v$  can be dropped. We now introduce a bilinear form

$$L(u, v) = \sum_{j=0}^{k-1} \{v_{4j+1}u_{4j+4} + v_{4j+3}u_{4j+2}\},$$

so that  $L(v, v) = P(v)$  and  $B(u, v) = L(u, v) + P(v)$ . We can then deduce the following expression for  $e(S, T)$ .

**Lemma 13** *For any  $S, T \subseteq \mathcal{U}$  we write  $s = \#S$  and*

$$\sigma = \sum_{u \in S} u, \quad \tau = \sum_{u \in T} u.$$

*We then have  $(-1)^{e(S)}(-1)^{e(T)} = (-1)^{e(S \triangle T)}(-1)^{e(S, T)}$ , where*

$$e(S, T) = s \sum_{u \in T} P(u) + L(\sigma, \tau).$$

Of course  $e(S, T)$  must in fact be symmetric in  $S$  and  $T$ , although this is not immediately apparent from Lemma 13.

We now write

$$\Sigma_{\mathcal{U}} = \sum_{S \subseteq \mathcal{U}: s \equiv h_0 \pmod{2}} (-1)^{e(S)},$$

so that (12) becomes

$$c_{k, h} = 2^{1-4^k} \sum_{\mathcal{U}} \left(\frac{2}{h}\right)^{R(\mathcal{U})} \Sigma_{\mathcal{U}}, \quad (14)$$

and we observe that

$$\Sigma_{\mathcal{U}}^2 = \sum_{S, S'} (-1)^{e(S)} (-1)^{e(S')} = \sum_{S, S'} (-1)^{e(S \triangle S')} (-1)^{e(S', S)}.$$

Now  $T = S \triangle S'$  runs over subsets of  $\mathcal{U}$  of even cardinality, and

$$e(S', S) = e(S \triangle T, S) = (\#(S \triangle T)) \left( \sum_{u \in S} P(u) \right) + L(\sigma + \tau, \sigma),$$

since

$$\sum_{u \in S \triangle T} u = \sum_{u \in S} u + \sum_{u \in T} u = \sigma + \tau.$$

Similarly we will have  $\#(S \triangle T) \equiv s + t \equiv s \pmod{2}$ , since  $t$  is even. At this point we observe that, according to Lemma 7,  $\mathcal{U}$  is a coset of a subspace,  $\mathcal{U}_0$ , say, on which  $P$  vanishes. Thus if  $s$  is even then  $\sigma \in \mathcal{U}_0$ , and hence  $L(\sigma, \sigma) = P(\sigma) = 0$ . To handle the case in which  $s$  is odd we shall use the identity

$$P(u + v + w) = P(u + v) + P(u + w) + P(v + w) + P(u) + P(v) + P(w),$$

which implies that

$$P(u + v + w) = P(u) + P(v) + P(w),$$

whenever  $u, v$  and  $w$  lie in an unlinked set  $\mathcal{U}$ . It follows by induction that

$$P(\sigma) = \sum_{u \in S} P(u)$$

whenever  $s$  is odd. From this we may deduce that

$$s \left( \sum_{u \in S} P(u) \right) + L(\sigma, \sigma) = 0,$$

whether  $s$  is even or odd. We therefore have

$$(-1)^{e(S, S \triangle T)} = (-1)^{L(\tau, \sigma)}.$$

It follows that

$$\Sigma_{\mathcal{U}}^2 = \sum_{T \subseteq \mathcal{U}: t \equiv 0 \pmod{2}} (-1)^{e(T)} \Sigma(T),$$

where

$$\Sigma(T) = \sum_{S \subseteq \mathcal{U}: s \equiv h_0 \pmod{2}} (-1)^{L(\tau, \sigma)}. \quad (15)$$

Now the right hand side of (15) is a sum of a multiplicative character over a coset under the symmetric difference operator. We therefore deduce that  $\Sigma(T) = 0$  unless the character is constant on the coset. Thus  $\Sigma(T) = 0$  unless  $L(\tau, \sigma) = 0$  whenever  $s$  is even. Let  $\mathcal{U}$  be the coset  $c + \mathcal{U}_0$ . Since there are  $2^{2^{2k}-1}$  subsets  $S$  whose cardinality has a prescribed parity, it follows that

$$\Sigma_{\mathcal{U}}^2 = 2^{2^{2k}-1} \sum_{T \in \mathcal{T}} (-1)^{e(T) + h_0 L(\tau, c)},$$

where  $\mathcal{T}$  is the set of all subsets  $T$  of  $\mathcal{U}$  of even cardinality, for which  $L(\tau, \sigma) = 0$  whenever  $s$  is even. It follows that  $\mathcal{T}$  is a subgroup under the symmetric difference operator. Moreover, for  $T \in \mathcal{T}$ , Lemma 13 implies that

$$(-1)^{e(T) + h_0 L(\tau, c)}$$

is a multiplicative character. Thus  $\Sigma_{\mathcal{U}}$  will vanish unless

$$e(T) = h_0 L(\tau, c)$$

for all  $T \in \mathcal{T}$ . In particular we have the following condition.

**Lemma 14** *Let  $\mathcal{U} = c + \mathcal{U}_0$ . Then  $\Sigma_{\mathcal{U}} = 0$  unless  $e(T)$  vanishes for any subset  $T$  of  $\mathcal{U}$  with  $t$  even and  $\tau = 0$ .*



We proceed to deduce a more useful criterion for  $\Sigma_{\mathcal{U}}$  to be non-vanishing. If  $s$  is odd then we may take  $T = S \triangle \{\sigma\}$  in Lemma 14. Note that  $\sigma \in \mathcal{U}$ , since  $s$  is odd. Now Lemma 14 implies that  $e(T) = 0$ , and Lemma 13 yields

$$(-1)^{e(S)} = (-1)^{Q(\sigma)},$$

since  $e(\{\sigma\}) = Q(\sigma)$  and

$$e(S, \{\sigma\}) = sP(\sigma) + L(\sigma, \sigma) = (s+1)P(\sigma) = 0.$$

Similarly if  $s$  is even and  $\sigma \neq 0$ , we may use  $T = S \triangle \{c, c + \sigma\}$ . This time

$$e(\{c, c + \sigma\}) = Q(c) + Q(c + \sigma) + B(c, c + \sigma).$$

We now define a symmetric bilinear form

$$\begin{aligned} Q(u, v) &= Q(u + v) - Q(u) - Q(v) \\ &= \sum_{j=0}^{k-1} (u_{4j+2}v_{4j+3} + u_{4j+3}v_{4j+4} + v_{4j+2}u_{4j+3} + v_{4j+3}u_{4j+4}), \end{aligned}$$

so that

$$(-1)^{Q(c)+Q(c+\sigma)} = (-1)^{Q(\sigma, c)+Q(\sigma)}.$$

Moreover  $B(c, c + \sigma) = B(c + \sigma, c)$ , by (13). As  $\sigma \in \mathcal{U}_0$ , we therefore have

$$B(c, c + \sigma) = B(c + \sigma, c) = P(c) + L(c + \sigma, c).$$

However

$$L(c + \sigma, c) = L(c, c) + L(\sigma, c) = P(c) + L(\sigma, c),$$

whence

$$B(c, c + \sigma) = L(\sigma, c).$$

It follows that

$$(-1)^{e(\{c, c+\sigma\})} = (-1)^{Q(\sigma)+M(\sigma, c)}, \quad (16)$$

where  $M$  is the bilinear form given by

$$\begin{aligned} M(u, v) &= Q(u, v) + L(u, v) \\ &= \sum_{j=0}^{k-1} (u_{4j+3}v_{4j+2} + u_{4j+3}v_{4j+4} + u_{4j+4}v_{4j+1} + u_{4j+4}v_{4j+3}). \end{aligned}$$

On the other hand  $T = S \triangle \{c, c + \sigma\}$  has  $t$  even and  $\tau = 0$ , so that  $e(T)$  vanishes, by Lemma 14. Then Lemma 13 yields

$$(-1)^{e(S)} = (-1)^{e(\{c, c+\sigma\})+L(\sigma, \sigma)}.$$

Here  $s$  even implies that  $\sigma \in \mathcal{U}_0$ . Thus  $L(\sigma, \sigma) = P(\sigma)$  will vanish automatically. Finally then, when  $s$  is even and  $\sigma \neq 0$ , we see that

$$(-1)^{e(S)} = (-1)^{Q(\sigma) + M(\sigma, c)}.$$

Moreover  $e(S) = 0$  if  $s$  is even and  $\sigma = 0$ , as in Lemma 14. We conclude that

$$(-1)^{e(S)} = (-1)^{Q(\sigma) + (1+s)M(\sigma, c)}, \quad (17)$$

in every case.

Taking subsets  $S$  and  $T$  for which  $s$  and  $t$  are even, a comparison of (17) with Lemma 13 shows that

$$Q(\sigma) + M(\sigma, c) + Q(\tau) + M(\tau, c) = Q(\sigma + \tau) + M(\sigma + \tau, c) + L(\sigma, \tau).$$

It follows that

$$M(\sigma, \tau) = Q(\sigma, \tau) + L(\sigma, \tau) = 0.$$

Now any non-zero  $\sigma \in \mathcal{U}_0$  arises from an admissible set  $S = \{c, \sigma + c\} \subseteq \mathcal{U}$ , and similarly for  $\tau$ . It follows that the bilinear form  $M$  must vanish identically on  $\mathcal{U}_0$ , providing only that  $\Sigma_{\mathcal{U}}$  is non-zero. Moreover in this case (17) will hold. We therefore define  $\mathcal{U}_0$  to be ‘good’ if the bilinear form  $M$  vanishes identically on  $\mathcal{U}_0$ . Thus  $\Sigma_{\mathcal{U}} = 0$  unless  $\mathcal{U}_0$  is good. Moreover (17) holds whenever  $\Sigma_{\mathcal{U}} \neq 0$ .

We proceed to show that (17) holds if  $M$  vanishes on  $\mathcal{U}_0$ , whether  $\Sigma_{\mathcal{U}}$  is zero or not. We do this by induction on  $s$ , the result being trivial if  $s$  is 0 or 1, and being given by (16) when  $s = 2$ . For a set  $S$  with  $s > 1$  we can write  $S = S' \triangle T$  with  $\#S' = s - 2$ ,

$$\sum_{u \in S'} u = \sigma',$$

and  $t = 2$ . Then Lemma 13, together with our induction hypothesis, applied to both  $S'$  and  $T$ , yields

$$\begin{aligned} e(S) &= Q(\sigma') + (1+s)M(\sigma', c) + Q(\tau) + M(\tau, c) + e(T, S') \\ &= Q(\sigma') + (1+s)M(\sigma', c) + Q(\tau) + M(\tau, c) + L(\tau, \sigma'). \end{aligned}$$

However  $\sigma' = \sigma + \tau$ , and  $\tau \in \mathcal{U}_0$ , so that

$$Q(\sigma') + Q(\tau) = Q(\sigma) + Q(\tau, \sigma),$$

$$(1+s)M(\sigma', c) + M(\tau, c) = (1+s)M(\sigma, c) + sM(\tau, c),$$

and

$$L(\tau, \sigma') = L(\tau, \sigma) + L(\tau, \tau) = L(\tau, \sigma) + P(\tau) = L(\tau, \sigma).$$

It follows that

$$e(S) = Q(\sigma) + (1+s)M(\sigma, c) + sM(\tau, c) + M(\tau, \sigma). \quad (18)$$

However, if  $s$  is even then  $\sigma \in \mathcal{U}_0$ , so that  $M(\tau, \sigma)$  vanishes, by our hypothesis. On the other hand, if  $s$  is odd then  $c + \sigma \in \mathcal{U}_0$ , so that

$$M(\tau, c) + M(\tau, \sigma) = M(\tau, c + \sigma) = 0.$$

Thus, whether  $s$  is even or odd, we may deduce from (18) that

$$e(S) = Q(\sigma) + (1 + s)M(\sigma, c),$$

as required for our induction argument.

We may now conclude as follows.

**Lemma 15** *Say that the subspace  $\mathcal{U}_0$  is ‘good’ if the bilinear form  $M$  vanishes identically on  $\mathcal{U}_0$ . Then  $\Sigma_{\mathcal{U}} = 0$  unless  $\mathcal{U}_0$  is good. Moreover, if  $\mathcal{U}_0$  is good then*

$$(-1)^{e(S)} = (-1)^{Q(\sigma) + (1+s)M(\sigma, c)}$$

for every  $S \subseteq \mathcal{U}$ .

## 7 Computation of $c_{k,h}$ —Completion of the Calculation

We have now to find out which subspaces  $\mathcal{U}_0$  are good. We write  $\mathbb{Z}_2^{4k}$  as a direct sum  $X \oplus Y$ , where

$$X = \{u \in \mathbb{Z}_2^{4k} : u_{4j+1} = u_{4j+3}, u_{4j+2} = u_{4j+4}, (0 \leq j < k)\}$$

and

$$Y = \{u \in \mathbb{Z}_2^{4k} : u_{4j+3} = u_{4j+4} = 0, (0 \leq j < k)\}.$$

We write  $u \in \mathbb{Z}_2^{4k}$  as  $u = x + y$  accordingly, and we define projections  $\pi_X(u) = x$  and  $\pi_Y(u) = y$ . It follows that

$$M(u, v) = M(\pi_X(u), \pi_Y(v))$$

for all  $u, v \in \mathcal{U}_0$ . If we now set  $\mathcal{U}_X = \pi_X(\mathcal{U}_0)$  and  $\mathcal{U}_Y = \pi_Y(\mathcal{U}_0)$ , then  $\mathcal{U}_0 \subseteq \mathcal{U}_X \oplus \mathcal{U}_Y$ . Moreover  $M$  must vanish on  $\mathcal{U}_X \oplus \mathcal{U}_Y$ . The map

$$\theta : x \rightarrow M(x, *),$$

from  $X$  into the dual of  $Y$ , takes  $\mathcal{U}_X$  into the annihilator  $U_Y^\circ$ . Moreover it is one-to-one, since if  $u_i = 0$  for every index  $i$  apart from  $i = 4j + 2$ , then  $M(x, u) = 0$  would imply  $x_{4j+1} = x_{4j+3} = 0$ , and similarly for  $x_{4j+2} = x_{4j+4} = 0$ . It follows that

$$\dim(\mathcal{U}_X) \leq 2k - \dim(\mathcal{U}_Y).$$

However

$$\dim(\mathcal{U}_X \oplus \mathcal{U}_Y) \geq \dim(\mathcal{U}_0) = 2k,$$

whence we deduce that

$$\mathcal{U}_0 = \mathcal{U}_X \oplus \mathcal{U}_Y, \quad (19)$$

and moreover that

$$\theta : \mathcal{U}_X \cong \mathcal{U}_Y^\circ. \quad (20)$$

Conversely, given subspaces of  $X$  and  $Y$  satisfying (20) it is easy to check that (19) produces a subspace  $\mathcal{U}_0$  of  $\mathbb{Z}_2^{4k}$  on which  $M$  vanishes. Notice in particular that  $\mathcal{U}_X$  determines  $\mathcal{U}_Y$ , by (20).

We shall now consider the condition that the quadratic form  $R$  is constant on the coset  $c + \mathcal{U}_0$ . Clearly the constant value must be  $R(c)$ . In view of (19) we see that  $R(c + u) = R(c)$  on each of  $\mathcal{U}_X$  and  $\mathcal{U}_Y$ . However  $R$ , regarded as a form on  $X$ , is clearly non-singular in the sense of Lemma 8, which therefore shows that  $\mathcal{U}_X$  can have dimension at most  $k$ . Similarly we see that  $\dim(\mathcal{U}_Y) \leq k$ . Hence (19) yields

$$\dim(\mathcal{U}_X) = \dim(\mathcal{U}_Y) = k.$$

We observe also that  $Y$  contains a  $k$ -dimensional subspace

$$\{u : u_{4j+2}, u_{4j+3}, u_{4j+4} = 0, \quad (0 \leq j < k)\}$$

on which  $R$  vanishes, and also contains a  $k$ -dimensional subspace  $\mathcal{U}_Y$  on which  $R(c + u) = R(c)$ . According to Lemma 10 we must therefore have  $R(c) = 0$ .

Finally we show that if  $R(c + u) = R(c)$  on  $\mathcal{U}_X$ , then automatically we have  $R(c + u) = R(c)$  for any  $u \in \mathcal{U}$ . To prove this we observe that

$$\begin{aligned} R(x, x') &= (R(c + x + x') - R(c)) - (R(c + x) - R(c)) - (R(c + x') - R(c)) \\ &= 0 \end{aligned}$$

for any  $x, x' \in \mathcal{U}_X$ . However

$$R(x, x') = M(x, \phi(x'))$$

for any  $x, x' \in X$ , where  $\phi : V \rightarrow Y$  is given by

$$\phi(x) = (x_1, x_2, 0, 0, x_5, x_6, 0, 0, \dots).$$

We therefore deduce that  $M(x, \phi(x')) = 0$  whenever  $x, x' \in \mathcal{U}_X$ , so that the map  $\theta$  considered above takes  $\mathcal{U}_X$  into the annihilator of  $\phi(\mathcal{U}_X)$ . Since  $\phi$  is clearly an isomorphism on  $X$ , we conclude that  $\phi(\mathcal{U}_X) = \mathcal{U}_Y$ . It then follows that  $\phi(c + \mathcal{U}) = \phi(c + \mathcal{U}_X)$ . Now, since  $R(v) = R(\phi(v))$ , we see that  $R(c + u)$  is constant on  $\mathcal{U}$ , providing only that it is constant on  $\mathcal{U}_X$ .

We can summarize these conclusions as follows.

**Lemma 16** *Let  $c \in \mathbb{Z}_2^{4k}$ . If there is any good  $2k$ -dimensional subspace  $\mathcal{U}_0$  of  $\mathbb{Z}_2^{4k}$  on which  $R(c + \mathcal{U}_0)$  is constant, then  $R(c)$  must vanish. If  $R(c) = 0$ , there is a one-to-one correspondence between such subspaces  $\mathcal{U}_0$ , and the set of  $k$ -dimensional subspaces  $\mathcal{U}_X$  of  $X$ , on which  $R(c + u)$  is constant.*

We may now rewrite (14) using Lemmas 15 and 16. It is convenient to count cosets  $c + \mathcal{U}$  for all  $c \in \mathbb{Z}_2^{4k}$ , so that each coset appears  $2^{2k}$  times. With this understanding the formula (14) becomes

$$c_{k,h} = 2^{1-4^k-2k} \sum_c \sum_{\mathcal{U}_X} \sum_{S \subseteq \mathcal{U}: s \equiv h_0 \pmod{2}} (-1)^{Q(\sigma) + (1+h_0)M(\sigma,c)}.$$

Here  $c$  is restricted by the condition  $R(c) = 0$ , and  $\mathcal{U}_X$  by the condition that  $R(c + u) = R(c)$  on  $\mathcal{U}_X$ . Since the map which takes  $S$  to  $\sigma$  is a homomorphism, each possible value of  $\sigma$  must arise equally often. When  $h_0 = 0$  the variable  $\sigma$  runs over the set  $\mathcal{U}_0$ , and if  $h_0 = 1$  it will run over  $\mathcal{U}$ . It therefore follows that

$$c_{k,h} = 2^{-4k} \sum_c \sum_{\mathcal{U}_X} \sum_{\sigma \in \mathcal{U}_0} (-1)^{Q(\sigma) + M(\sigma,c)}$$

when  $h_0 = 0$ , and

$$c_{k,h} = 2^{-4k} \sum_c \sum_{\mathcal{U}_X} \sum_{\sigma \in \mathcal{U}_0} (-1)^{Q(c+\sigma)}$$

when  $h_0 = 1$ .

We may decompose  $c$  as a sum of two vectors  $c' = \phi(c)$  and  $c'' = c - c'$ . Then  $R(c) = R(c')$  and  $R(c + u) = R(c' + u)$ , so that we can interchange the orders of summation to give

$$\sum_c \sum_{\mathcal{U}_X} \sum_{\sigma} = \sum_{c'} \sum_{\mathcal{U}_X} \sum_{\sigma} \sum_{c''}.$$

However

$$\sum_{c''} (-1)^{Q(\sigma) + M(\sigma,c)} = (-1)^{Q(\sigma) + M(\sigma,c')} \sum_{c''} (-1)^{M(\sigma,c'')}.$$

The sum on the right is over an additive subgroup of  $Z^{4k}$ , and the summand is a multiplicative character which is identically 1 if and only if  $\sigma \in Y$ . The latter case occurs precisely when  $\sigma \in \mathcal{U}_Y$ , so that there are  $2^k$  possible values of  $\sigma$ . Moreover, for such  $\sigma$  we will have

$$(-1)^{Q(\sigma)} = (-1)^{M(\sigma,c')} = 1.$$

It therefore follows that

$$\sum_{\sigma \in \mathcal{U}_0} \sum_{c''} (-1)^{Q(\sigma) + M(\sigma,c)} = 2^{3k}.$$

Similarly we find that

$$\begin{aligned}
\sum_{c''} (-1)^{Q(c+\sigma)} &= \prod_{j=0}^k \left( \sum_{a,b \pmod{2}} (-1)^{(a+c_{4j+3}+\sigma_{4j+3})(b+c_{4j+2}+\sigma_{4j+2}+\sigma_{4j+4})} \right) \\
&= \prod_{j=0}^k \left( \sum_{a,b \pmod{2}} (-1)^{ab} \right) \\
&= 2^k,
\end{aligned}$$

whence

$$\sum_{\sigma \in \mathcal{U}_0} \sum_{c''} (-1)^{Q(c+\sigma)} = 2^{3k}.$$

We therefore see that

$$c_{k,h} = 2^{-k} \# \{(c', \mathcal{U}_X)\}.$$

According to Lemma 9 there are  $2^{2k-1} + 2^{k-1}$  available vectors  $c$ , so that, to complete the proof of Theorem 1, it suffices to show that there are

$$\prod_{j=0}^{k-1} (1 + 2^j)$$

possible spaces  $\mathcal{U}_X$  corresponding to each admissible  $c'$ . In view of Lemma 11 it will be enough if we can show that the form  $R_{c'}$ , defined in analogy with (6), is equivalent to  $P^{(k)}$  under a suitable linear transformation.

However  $R_{c'}$  is composed of  $k$  blocks of the type

$$c_1 x^2 + xy + c_2 y^2.$$

If  $c_1 = c_2 = 0$  this is already of the shape  $xy$ . If  $c_1 = 1$  and  $c_2 = 0$  then we replace  $y$  by  $y' = x + y$  to get  $xy'$ , and similarly if  $c_1 = 0$  and  $c_2 = 1$ . If we have two blocks of the form

$$x^2 + xy + y^2, \quad z^2 + zw + w^2$$

we can substitute

$$x = x' + z' + w', \quad y = x' + y', \quad z = x' + y' + z', \quad w = x' + y' + w'$$

to get  $x'y' + z'w'$ . Hence  $R_{c'}$  can be transformed into  $P(k)$  providing that there are an even number of blocks with  $c_1 = c_2 = 1$ . This last criterion can of course be written in the form

$$\sum_{j=0}^{k-1} c_{4j+1} c_{4j+2} = 0,$$

which is exactly the condition  $R(c') = 0$ . This completes the proof of Theorem 1.

## 8 Proof of Theorem 2

We begin this section with the following result.

**Lemma 17** *Let non-negative real numbers  $C_0, C_1, \dots$  be given, satisfying*

$$C_k \ll 2^{k(k+1)/2}.$$

*Then there is at most one solution of the equations*

$$\sum_{s=0}^{\infty} x_s 4^{sk} = C_k, \quad (k = 0, 1, \dots) \quad (21)$$

*in non-negative real numbers  $x_s$ .*

For the proof we shall use the function

$$G(z) = \prod_{n=0}^{\infty} \left(1 - \frac{z}{4^n}\right).$$

The product is clearly absolutely convergent for any complex  $z$ , and so defines an entire function, satisfying  $G(4z) = (1 - 4z)G(z)$ . Thus if  $G$  has a Taylor expansion  $\sum a_n z^n$ , the coefficients must satisfy

$$4^n a_n = a_n - 4a_{n-1}, \quad (n \geq 1).$$

It then follows by induction that

$$a_n = (-1)^n \frac{4^n}{\prod_{j=1}^n (4^j - 1)}, \quad (22)$$

and hence that

$$a_n \ll 2^{n-n^2}.$$

By our hypothesis on the size of the  $C_k$  we conclude that  $\sum_{n=0}^{\infty} a_n C_n 4^{-nK}$  converges absolutely, for any positive integer  $K$ . Since the unknowns  $x_s$  in (21) are to be non-negative, it follows that the double sum

$$\sum_{n=0}^{\infty} \sum_{s=0}^{\infty} a_n x_s 4^{(s-K)n}$$

must converge absolutely. We therefore deduce that

$$\begin{aligned} \sum_{n=0}^{\infty} a_n C_n 4^{-nK} &= \sum_{n=0}^{\infty} \sum_{s=0}^{\infty} a_n x_s 4^{(s-K)n} \\ &= \sum_{s=0}^{\infty} \sum_{n=0}^{\infty} a_n x_s 4^{(s-K)n} \\ &= \sum_{s=0}^{\infty} x_s G(4^{s-K}). \end{aligned} \quad (23)$$

However we have  $G(4^t) = 0$  for any non-negative integer  $t$ , whence (23) yields

$$\sum_{n=0}^{\infty} a_n C_n 4^{-nK} = \sum_{s=0}^{K-1} x_s G(4^{s-K}).$$

This formula can be used with  $K = 1, 2, \dots$  to obtain the values of  $x_0, x_1, x_2, \dots$  successively. This completes the proof of Lemma 17.

**Lemma 18** *Let  $c_k$  and  $d_r$  be as in Theorems 1 and 2. Then the equations*

$$\sum_{s=0}^{\infty} x_s 4^{sk} = c_k, \quad (k = 0, 1, \dots) \quad (24)$$

*are satisfied by  $x_s = d_{2s}$  and no other set of non-negative values. Similarly the equations*

$$\sum_{s=0}^{\infty} x_s 2^{(2s+1)k} = c_k, \quad (k = 0, 1, \dots) \quad (25)$$

*are satisfied by  $x_s = d_{2s+1}$  and no other set of positive values.*

We begin the proof of Lemma 18 by noting the identity

$$\prod_{m=0}^{\infty} \left(1 + \frac{x}{2^m}\right) = \sum_{m=0}^{\infty} x^m \frac{2^m}{(2-1)(2^2-1)\dots(2^m-1)}.$$

This follows by exactly the same reasoning as was used to obtain (22) in the proof of the previous lemma. We therefore see that

$$\lambda \prod_{m=0}^{\infty} \left(1 + \frac{x}{2^m}\right) = \sum_{m=0}^{\infty} d_m x^m,$$

with  $\lambda$  and  $d_m$  as in Theorem 2. If we denote the left hand side of the above expression by  $F(x)$  then it is apparent that  $F(-2^k) = 0$  for any non-negative integer  $k$ . Moreover

$$\prod_{m=0}^{\infty} (1 + 2^{k-m}) = \left( \prod_{m=k}^{\infty} (1 + 2^{k-m}) \right) \left( \prod_{m=0}^{k-1} (1 + 2^{k-m}) \right) = 2\lambda^{-1} c_k,$$

whence  $F(2^k) = 2c_k$ . We therefore see that

$$\sum_{s=0}^{\infty} d_{2s} 2^{2sk} = \frac{1}{2} (F(2^k) + F(-2^k)) = c_k,$$

and

$$\sum_{s=0}^{\infty} d_{2s+1} 2^{(2s+1)k} = \frac{1}{2} (F(2^k) - F(-2^k)) = c_k.$$



This shows that the equations (24) and (25) are indeed satisfied by  $d_{2s}$  and  $d_{2s+1}$  respectively.

It remains to show that these solutions are unique. Equations (24) are already in the form considered in Lemma 17, and equations (25) will also be of the required form once we have divided through by  $2^k$ . It follows that each  $x_s$  is uniquely determined, and can only take the values claimed in Lemma 18.

We can now complete the proof of Theorem 2. We write

$$d_s(X) = \frac{\#\{D \in S(X, h) : s(D) = r\}}{\#S(X, h)},$$

so that Theorem 1 becomes

$$\sum_{r=0}^{\infty} d_{2r}(X) 2^{2rk} = c_k + o_k(1) \quad (k = 0, 1, \dots) \quad (26)$$

for  $h = 1$  or  $3$ , and

$$\sum_{r=0}^{\infty} d_{2r+1}(X) 2^{(2r+1)k} = c_k + o_k(1) \quad (k = 0, 1, \dots)$$

otherwise. Clearly  $0 \leq d_s(X) \leq 1$  for any  $s$  and any  $X$ , so  $d_0(X)$  must have at least one limit point,  $d'_0$  say. If

$$d_0(X_n) \rightarrow d'_0$$

the values of  $d_2(X_n)$  form an infinite bounded set, and hence have at least one limit point,  $d'_2$ , say. There is therefore a subsequence  $X_{n_m}$  for which

$$d_{2r}(X_{n_m}) \rightarrow d'_{2r} \quad (r = 0, 1).$$

Repeating the argument we get an infinite series of subsequences, from which we can use the standard diagonal process to select a further subsequence,  $Y_n$  say, such that

$$d_{2r}(Y_n) \rightarrow d'_{2r} \quad (r = 0, 1, \dots).$$

We claim that

$$\sum_{r=0}^{\infty} d'_{2r} 2^{2rk} = c_k \quad (k = 0, 1, \dots). \quad (27)$$

To prove this we fix  $k$ , and take an arbitrary  $\varepsilon > 0$ . In view of (26), together with the fact that  $c_m \ll 2^{m(m+1)/2}$ , we see that

$$d_{2r}(Y_n) \ll 2^{-2rm+m(m+1)/2}.$$

The choice  $m = 2r$  therefore yields

$$d_{2r}(Y_n) \ll 2^{r-2r^2}$$

uniformly in  $n$ . It follows that there exists a value of  $R(k, \varepsilon)$  such that

$$\sum_{r>R} d_{2r}(Y_n) 2^{2rk} < \varepsilon$$

for any  $R \geq R(k, \varepsilon)$ , uniformly in  $n$ . We may now take  $n \rightarrow \infty$  in the inequality

$$\left| \sum_{r=0}^R d_{2r}(Y_n) 2^{2rk} - c_k \right| < \varepsilon$$

to deduce that

$$\left| \sum_{r=0}^R d'_{2r} 2^{2rk} - c_k \right| < \varepsilon$$

for any  $R \geq R(k, \varepsilon)$ . The claimed relation (27) then follows.

We can now use Lemma 18 to deduce that  $d'_0 = d_0$ . However  $d'_0$  was an arbitrary limit point of  $d_0(X)$ , so that we must have  $d_0(X) \rightarrow d_0$  as  $X$  goes to infinity. It then follows from (26) that

$$d_0 + \sum_{r=1}^{\infty} d_{2r}(X) 2^{2rk} = c_k + o_k(1) \quad (k = 0, 1, \dots).$$

We may now repeat the argument to show that  $d_2(X)$  must tend to  $d_2$ , and so on. Moreover a similar argument can be used to handle  $d_{2r+1}(X)$ . This completes our discussion of Theorem 2.

## 9 The Corollaries

To prove Corollary 1 we begin by showing that

$$\sum_{s \geq r, s \text{ odd}} d_s \leq (1.7313\dots) 2^{-(r^2-r)/2}, \quad (28)$$

and similarly for  $s$  even. If  $s = S$  is the first available value, the sum will be

$$d_S \sum_{k=0}^{\infty} \frac{4^k}{\prod_{1 \leq j \leq 2k} (2^{S+j} - 1)}.$$

The sum is decreasing with  $S$ , and so is maximal when  $S = 1$ . On the other hand the above reasoning also gives

$$\sum_{s \geq 1, s \text{ odd}} d_s = d_1 \sum_{k=0}^{\infty} \frac{4^k}{\prod_{1 \leq j \leq 2k} (2^{1+j} - 1)}.$$

However the case  $k = 0$  of (25) shows that the left hand side is just  $c_0 = 1$ . We therefore deduce that

$$\sum_{s \geq r, s \text{ odd}} d_s \leq d_S d_1^{-1},$$

and similarly for  $s$  odd. Now

$$d_S d_1^{-1} = \frac{2^{S-1}}{\prod_{1 \leq j \leq S} (2^j - 1)} \leq 2^{-(S^2-S)/2} (2 \prod_{j=1}^{\infty} (1 - 2^{-j}))^{-1}.$$

Since  $S \geq r$  and

$$(2 \prod_{j=1}^{\infty} (1 - 2^{-j}))^{-1} = 1.7313 \dots$$

the result (28) follows.

Now

$$\frac{\#\{D \in S(X, h); s(D) \geq r\}}{\#S(X, h)} = 1 - \frac{\#\{D \in S(X, h); s(D) < r\}}{\#S(X, h)}.$$

Since  $r$  is fixed we can apply Theorem 2 to each value of  $s(D)$  on the right to obtain

$$1 - \sum_{s < r, s \text{ odd}} d_s = \sum_{s \geq r, s \text{ odd}} d_s,$$

as the limit for  $h = 5$  or  $7$ , and similarly for  $h = 1$  or  $3$ . The corollary then follows. The reader will observe that the constant  $1.7313 \dots$  is by no means best possible, although it cannot be reduced below  $1.5$ .

For the proof of Corollary 2 we consider the case in which  $h = 1$  or  $3$ , and  $s = s(D)$  is even, the alternative case being similar. We begin by showing that

$$\sum_{s \text{ even}} s d_s = c'. \quad (29)$$

To do this shall use the function

$$F(x) = \lambda \prod_{m=0}^{\infty} (1 + \frac{x}{2^m}) = \sum_{m=0}^{\infty} d_m x^m,$$

introduced in the previous section. We have

$$\sum_{s \text{ even}} s d_s = (F'(1) - F'(-1))/2.$$

However  $F(1) = 1$ , and

$$\frac{F'(1)}{F(1)} = \sum_{m=0}^{\infty} \frac{1}{2^m + 1}.$$

Moreover

$$F(x) = (1+x)\lambda \prod_{m=1}^{\infty} \left(1 + \frac{x}{2^m}\right),$$

so that

$$F'(-1) = \lambda \prod_{m=1}^{\infty} (1 - 2^{-m}) = \prod_{m=1}^{\infty} \left(\frac{1 - 2^{-m}}{1 + 2^{-m}}\right).$$

These expressions then produce (29), in view of the definition of  $c'$ .

To deduce Corollary 2 we begin by choosing an arbitrary positive  $\varepsilon$ . Then Theorem 1, with  $k = 1$ , shows that there exists an absolute constant  $X_0$ , such that

$$\sum_{D \in S(X, h)} 2^{s(D)} < 4\#S(X, h),$$

for  $X \geq X_0$ . We choose  $r = r(\varepsilon)$  such that  $2^{r/2} > 8\varepsilon^{-1}$ . Then

$$s/2 \leq 2^{s/2} \leq 2^{-r/2} \cdot 2^s < \frac{\varepsilon}{8} 2^s$$

for  $s > r$ , so that

$$\sum_{D \in S(X, h), s(D) > r} s(D) < \varepsilon \#S(X, h).$$

On the other hand, since  $r$  is fixed, Theorem 2 yields

$$\sum_{D \in S(X, h), s(D) \leq r} s(D) \sim \left( \sum_{s \leq r, \text{ seven}} sd_s \right) \#S(X, h)$$

for  $h = 1$  or  $3$ . If we now require  $r$  to be so large that

$$\sum_{s > r, s \text{ even}} sd_s > c' - \varepsilon,$$

we may deduce that

$$\left| \frac{\sum_{D \in S(X, h)} s(D)}{\#S(X, h)} - c' \right| < 2\varepsilon$$

if  $X$  is large enough, and Corollary 2 follows.

Finally we remark that Corollaries 3 and 4 are immediate consequences of Corollaries 1 and 2, in view of the inequality  $r(D) \leq s(D)$ .

## References

- [1] B.J. Birch and N.M. Stephens, The parity of the rank of the Mordell-Weil group, *Topology*, 5 (1966), 295-299.

- [2] B.J.Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves. II, *J. Reine Angew. Math.*, 218 (1965), 79-108.
- [3] A. Brumer and D.R. Heath-Brown, Average ranks of elliptic curves, II, to appear.
- [4] J.W.S. Cassels, Arithmetic of curves of genus 1. IV. Proof of the Hauptvermutung, *J. Reine Angew. Math.*, 211 (1962), 95-112.
- [5] D.R. Heath-Brown, The size of Selmer groups for the congruent number problem, *Invent. Math.*, 111 (1993), 171-195.

# Appendix

P. Monsky  
Mathematics Department, Brandeis University,  
Waltham, MA 02254

The purpose of this appendix is to give a simple proof of the following result.

**Theorem** *If  $D$  is a positive odd square-free integer then  $s(D)$  is even for  $D \equiv 1, 2$  or  $3 \pmod{8}$ , and odd for  $D \equiv 5, 6$  or  $7 \pmod{8}$ .*

This is the parity condition mentioned in the first paper [2] of this series. As described there, the parity condition yields stronger average bounds for  $s(D)$  than can otherwise be obtained. As described in the introduction, it is possible to extract this result from the work of Cassels [4] and Birch and Stephens [1]. However the proof given here seems to be of independent interest, firstly because it is entirely elementary, and secondly because the method can be applied to twists of other curves with rational 2-torsion, even when there is no complex multiplication.

We shall give the argument for odd  $D$  in detail, and then sketch the proof for even  $D$ . We write the equations (3) of [2] in the form

$$abx^2 + Dy^2 = az^2, \quad abx^2 - Dy^2 = bw^2, \quad (30)$$

where  $a$  and  $b$  are arbitrary positive divisors of  $D$ . (Then  $D_1 = ab/(a, b)$ ,  $D_2 = a/(a, b)$ ,  $D_3 = b/(a, b)$  and  $D_4 = D/(a, b)$ , in the notation of [2].) For each prime factor  $p$  of  $D$  the condition for solvability in  $\mathbb{Q}_p$  is as follows:

$$\begin{aligned} \left(\frac{a}{p}\right) &= \left(\frac{b}{p}\right) = 1, & \text{for } p \nmid a, p \nmid b, \\ \left(\frac{2D/a}{p}\right) &= \left(\frac{2b}{p}\right) = 1, & \text{for } p|a, p \nmid b, \\ \left(\frac{2a}{p}\right) &= \left(\frac{-2D/b}{p}\right) = 1, & \text{for } p \nmid a, p|b, \\ \left(\frac{D/a}{p}\right) &= \left(\frac{-D/b}{p}\right) = 1, & \text{for } p|a, p|b. \end{aligned}$$

We give the set  $G$  of divisors  $a$  of  $D$  a group structure by defining  $a * a' = aa'/(a, a')^2$ , so that  $G$  is isomorphic to  $C_2^n$ , where  $n = \Omega(D)$ . We can then define a homomorphism  $\phi_p : G \times G \rightarrow \{\pm 1\} \times \{\pm 1\}$ , by taking

$$\begin{aligned} \phi_p(a, b) &= \left(\left(\frac{a}{p}\right), \left(\frac{b}{p}\right)\right) \text{ for } p \nmid ab, \\ \phi_p(1, D) &= \left(\left(\frac{2}{p}\right), \left(\frac{-2}{p}\right)\right), \\ \phi_p(D, 1) &= \left(\left(\frac{2}{p}\right), \left(\frac{2}{p}\right)\right). \end{aligned}$$

Thus (1) is solvable in  $\mathbb{Q}_p$  precisely when  $(a, b)$  lies in the kernel of  $\phi_p$ . It follows that if  $K$  is the intersection of the kernels of the homomorphisms  $\phi_p$ , then  $K$  has size  $2^{s(D)}$ .

We transform this situation into one involving linear algebra over  $\mathbb{Z}_2^{2n}$ , by making the pair  $(a, b)$  correspond to the vector  $\mathbf{x} \in \mathbb{Z}_2^{2n}$ , where for  $i \leq n$  we have  $x_i = 1$  if and only if  $p_i | a$ , and  $x_{i+n} = 1$  if and only if  $p_i | b$ . Here  $p_1, \dots, p_n$  are the primes dividing  $D$ . We then produce a  $2n \times 2n$  matrix  $M$  whose kernel identifies with  $K$ . To describe  $M$  we define  $D_j$  to be the diagonal  $n \times n$  matrix whose  $i$ -th entry is 0 if  $(\frac{j}{p_i}) = 1$  and is 1 otherwise. Moreover we take  $A$  to be the  $n \times n$  matrix given by

$$A_{ij} = \begin{cases} 0 & (\frac{p_j}{p_i}) = 1, j \neq i, \\ 1 & (\frac{p_j}{p_i}) = -1, j \neq i, \end{cases}$$

and

$$A_{ii} = \sum_{j: j \neq i} A_{ij}.$$

Then a little thought shows that one can take

$$M = \left( \begin{array}{c|c} A + D_2 & D_2 \\ \hline D_2 & A + D_{-2} \end{array} \right).$$

We therefore have  $s(D) = 2n - \text{rank}(M)$ .

For an arbitrary matrix  $U$  we shall write  $\mathbf{r}(U)$  for the sum of the rows of  $U$ , and  $\mathbf{c}(U)$  for the sum of the columns. Note that  $\sum \mathbf{r}(U)_i = \sum \mathbf{c}(U)_i$ . We shall write  $\mathbf{u} = \mathbf{r}(D_{-1})$  and  $\mathbf{v} = \mathbf{r}(D_2)$ . Observe that  $\sum u_i = 0$  if and only if  $D \equiv 1 \pmod{4}$ , and  $\sum v_i = 0$  if and only if  $D \equiv \pm 1 \pmod{8}$ . Moreover

$$A + A^T = D_{-1} + \mathbf{u}^T \mathbf{u}, \quad (31)$$

where  $\mathbf{u}^T \mathbf{u}$  is a  $2n \times 2n$  matrix. Here the diagonal entries on both sides vanish, and the off-diagonal entries agree by the law of quadratic reciprocity.

We now apply the following result, which we shall prove later.

**Lemma** *Let  $U$  be an  $m \times m$  matrix, defined over an arbitrary field, and let  $\mathbf{r} = \mathbf{r}(U)$  and  $\mathbf{c} = \mathbf{c}(U)$ . Then if  $\mathbf{d}$  is any row vector with  $\sum d_i \neq 1$ , we have*

$$\text{rank}(U) = \text{rank}(U - \mathbf{c}\mathbf{d}).$$

Moreover, if  $\sum r_i = 1$ , then

$$\text{rank}(U) = 1 + \text{rank}(U - \mathbf{c}\mathbf{r}).$$

In order to apply the lemma to the matrix  $M$ , we observe that  $\mathbf{c}(A) = \mathbf{0}$ , by construction. Then (31) shows that  $\mathbf{r}(A)$  will be  $\mathbf{u}$  or  $\mathbf{0}$  according as  $D \equiv 1$  or  $3$

(mod 4). It follows that  $\mathbf{c}(M) = (\mathbf{0}, \mathbf{u})^T$ , so that we can take  $\mathbf{d} = (\mathbf{0}, \mathbf{u})$  in the lemma, providing that  $\sum u_i \neq 1$ . Thus, if

$$M_1 = \left( \begin{array}{c|c} A + D_2 & D_2 \\ \hline D_2 & A + D_{-2} + \mathbf{u}^T \mathbf{u} \end{array} \right),$$

then  $M$  and  $M_1$  will have the same rank, providing that  $D \equiv 1 \pmod{4}$ . In the alternative case we will have  $\mathbf{r}(M) = (\mathbf{0}, \mathbf{u})$ , and  $\sum \mathbf{r}(M)_i = 1$ , so that the second part of the lemma applies, and yields

$$\text{rank}(M) = 1 + \text{rank}(M_1).$$

We now relate the rank of  $M_1$  to that of a symmetric matrix. In view of (31) we have

$$M_1 = \left( \begin{array}{c|c} A + D_2 & D_2 \\ \hline D_2 & A^T + D_2 \end{array} \right),$$

and so

$$\left( \begin{array}{c|c} I & I \\ \hline I & 0 \end{array} \right) M_1 \left( \begin{array}{c|c} I & 0 \\ \hline I & I \end{array} \right) = \left( \begin{array}{c|c} A + A^T & A^T \\ \hline A & D_2 \end{array} \right) = M_2,$$

say. It follows that  $M_1$  and  $M_2$  have the same rank.

Finally we apply the lemma to  $M_2$ , taking  $\mathbf{d} = \mathbf{r}(M_2) = (\mathbf{0}, \mathbf{v})$ . Hence if

$$M_3 = M_2 - \left( \begin{array}{c|c} 0 & 0 \\ \hline 0 & \mathbf{v}^T \mathbf{v} \end{array} \right) = \left( \begin{array}{c|c} D_{-1} + \mathbf{u}^T \mathbf{u} & A^T \\ \hline A & D_2 + \mathbf{v}^T \mathbf{v} \end{array} \right)$$

we will have  $\text{rank}(M_2) = \text{rank}(M_3)$  if  $\sum v_i = 0$ , and  $\text{rank}(M_2) = 1 + \text{rank}(M_3)$  otherwise.

We are now ready to prove the theorem for odd values of  $D$ . We have seen that

$$s(D) = 2n - k - \text{rank}(M_3),$$

where

$$k = \begin{cases} 0 & D \equiv 1 \pmod{8}, \\ 1 & D \equiv 5 \text{ or } 7 \pmod{8}, \\ 2 & D \equiv 3 \pmod{8}. \end{cases}$$

It remains to observe that the rank of  $M_3$  is necessarily even. This is because  $M_3$  can be thought of as the matrix of an alternating bilinear form on a vector space over  $\mathbb{Z}_2$ . The vector space therefore decomposes into a direct sum of hyperbolic planes, together with a subspace on which the form is trivial. It follows that the form must have even rank.

We now present a sketch proof for the case in which  $D$  is positive, even and square-free. For convenience we shall write  $D_0 = D/2$ . Each equivalence class of rational points on  $X(X^2 - D^2) = Y^2$  modulo torsion contains exactly one



representative with  $X/D$  a 2-adic integer such that  $X/D \equiv 1 \pmod{4}$ . We then see that  $2^{s(D)}$  is the number of everywhere locally solvable systems

$$ax^2 + Dy^2 = bz^2, \quad ax^2 - Dy^2 = abw^2$$

with  $a|D_0$ ,  $b|D_0$ ,  $a \equiv 1 \pmod{4}$  and  $b > 0$ . As before it suffices to consider  $p$ -adic solubility for the various primes  $p|D_0$ . We let  $G'$  be the set of positive and negative divisors  $a \equiv 1 \pmod{4}$  of  $D_0$ , with the same group operation  $a * a' = aa'/(a, a')^2$  as before. One may then define homomorphisms  $\phi_p : G' \times G \rightarrow \{\pm 1\} \times \{\pm 1\}$  by

$$\begin{aligned} \phi_p(a, b) &= \left( \left( \frac{a}{p} \right), \left( \frac{b}{p} \right) \right) \text{ for } p \nmid ab, \\ \phi_p(1, D_0) &= \left( \left( \frac{-1}{p} \right), \left( \frac{2}{p} \right) \right), \\ \phi_p\left(\left(\frac{-1}{D_0}\right)D_0, 1\right) &= \left( \left( \frac{\alpha}{p} \right), \left( \frac{2}{p} \right) \right), \end{aligned}$$

where  $\alpha = -2$  for  $D_0 \equiv 1 \pmod{4}$  and  $\alpha = 2$  otherwise. Proceeding as before one finds that  $2^{s(D)}$  is the size of the kernel of the matrix

$$M = \left( \begin{array}{c|c} B + D_\alpha & D_{-1} \\ \hline D_2 & A + D_2 \end{array} \right).$$

Here  $B$  is defined analogously to  $A$  except that we have

$$B_{ij} = \begin{cases} 0 & \left( \frac{q_i}{p_i} \right) = 1, \\ 1 & \left( \frac{q_i}{p_i} \right) = -1, \end{cases}$$

for  $i \neq j$ , where  $q_j = \pm p_j \equiv 1 \pmod{4}$ . One now finds that  $B + D_\alpha = A^T + D_2$ , so that

$$s(D) = 2\Omega(D_0) - \text{rank}(M_1),$$

where

$$M_1 = \left( \begin{array}{c|c} D_2 & A + D_2 \\ \hline A^T + D_2 & D_{-1} \end{array} \right).$$

However

$$\left( \begin{array}{c|c} I & 0 \\ \hline I & I \end{array} \right) M_1 \left( \begin{array}{c|c} I & I \\ \hline 0 & I \end{array} \right) = \left( \begin{array}{c|c} D_2 & A \\ \hline A^T & A + A^T + D_{-2} \end{array} \right) = M_2,$$

say, and since  $M_2$  is symmetric, with  $\mathbf{r}(M_2) = (\mathbf{v}, \mathbf{u} + \mathbf{v})$ , the lemma yields

$$\text{rank}(M_1) = \text{rank}(M_2) = \text{rank}(M_2 - \mathbf{r}^T \mathbf{r}) + \delta,$$

where  $\delta = 0$  for  $D_0 \equiv 1 \pmod{4}$  and  $\delta = 1$  otherwise. As before  $M_2 - \mathbf{r}^T \mathbf{r}$  is the matrix of an alternating bilinear form and hence has even rank. The result then follows.

It remains to prove the lemma. We begin by observing that

$$\text{rank}(U) = \text{rank}(U|\mathbf{c}) = \text{rank}(U - \mathbf{cd}|\mathbf{c}).$$

Thus for the first assertion of the lemma it suffices to show that  $\mathbf{c}$  is in the column space of  $U - \mathbf{cd}$ . This however is immediate if  $\sum d_i \neq 1$ , since

$$(U - \mathbf{cd})\mathbf{w} = (1 - \sum d_i)\mathbf{c},$$

where  $\mathbf{w}$  is the column vector consisting of  $m$  1's.

For the second part of the lemma we need to prove that  $\mathbf{c}$  is not in the column space of  $U - \mathbf{cr}$ . However

$$\mathbf{w}^T(U - \mathbf{cr}) = \mathbf{r} - (\sum c_i)\mathbf{r} = \mathbf{0}$$

with  $\mathbf{w}$  as above, since

$$\sum c_i = \sum r_i = 1,$$

by hypothesis. Hence if

$$\mathbf{c} = (U - \mathbf{cr})\mathbf{x}$$

for any column vector  $\mathbf{x}$ , we would have

$$1 = \sum c_i = \mathbf{w}^T \mathbf{c} = \mathbf{w}^T(U - \mathbf{cr})\mathbf{x} = 0,$$

a contradiction. This completes the proof of the lemma.