SOME DENSITY RESULTS FOR NEGATIVE PELL EQUATIONS; AN APPLICATION OF GRAPH THEORY

J. E. CREMONA AND R. W. K. ODONI

0. *Introduction*

Let $\mathbb{Z}$ be the ring of integers, let $\mathbb{N} = \{n \in \mathbb{Z} : n > 0\}$ be the set of natural numbers, and let $\mathbb{Q}$ be the field of rationals. Now let $d \in \mathbb{N}$, $\sqrt{d} \notin \mathbb{Q}$. We shall obtain new results on the distribution of such d for which the *negative Pell equation*

$$x^2 - dy^2 = -1 \qquad (x, y \in \mathbb{Z}) \tag{0.1}$$

is soluble. There is a vast literature on (0.1) (see [**2**, **7**, **15**, **16**] for useful assessments of the known results). Whereas the *positive Pell equation* $x^2 - dy^2 = +1$ has been well understood since the eighteenth century, the situation with regard to (0.1) is still unsatisfactory, in that no simple rational necessary and sufficient criteria exist for deciding when it is soluble (see our remarks at the end of this introduction for a clarification of this assertion). Trivially, (0.1) is insoluble if $4 \mid d$ or if $p \mid d$ for some prime p in $\mathbb{N}$ with $p \equiv 3 \pmod 4$. Moreover, if (0.1) is soluble for d, it must be soluble for d_0, the maximal square-free divisor of d in $\mathbb{N}$. The converse is false, but Rédei [**18**] has given simple procedures for passing from the case d_0 to the case d, and so we shall restrict our attention to the case $d = d_0$ square-free. Let

$$\mathscr{D} = \{d > 1 \text{ in } \mathbb{N} : d \text{ square-free with no prime factor } p \equiv 3 \pmod 4 \text{ in } \mathbb{N}\},$$

and, for $n \in \mathbb{N}$, let $\mathscr{D}_n = \{d \in \mathscr{D} : d \text{ has exactly } n \text{ prime factors}\}$.

The main novelty in our approach is to associate canonically with each $d \in \mathscr{D}_n$ a graph $\gamma(d)$ on the vertices $\{1, 2, \ldots, n\}$. (Throughout this paper we use 'graph' to mean a labelled, undirected graph free of loops and multiple edges.) We isolate a particular class Ω_n of graphs on $\{1, 2, \ldots, n\}$ (called *odd graphs*), and show that $\gamma(d) \in \Omega_n$ is a sufficient condition on $d \in \mathscr{D}_n$ for (0.1) to be soluble (see §1). It turns out that the odd graphs are precisely those having an odd number of spanning trees. By means of the matrix-tree theorem [**10**] we are able to enumerate Ω_n in §2. In §3 we turn to the question of how $\gamma(d)$ varies with d, when $d \in \mathscr{D}_n$ ($n \in \mathbb{N}$ fixed), and $1 < d \leqslant X$ (X large). By means of results on the distribution of primes in arithmetic progressions we shall show in §3 that $\gamma(d)$ is 'asymptotically uniformly distributed' amongst the $2^{\binom{n}{2}}$ graphs on $\{1, 2, \ldots, n\}$, in the sense that

$$\lim_{X \to \infty} \frac{\#\{d \in \mathscr{D}_n : d \leqslant X, \gamma(d) = G\}}{\#\{d \in \mathscr{D}_n : d \leqslant X\}} = 2^{-\binom{n}{2}} \tag{0.2}$$

for each fixed $n \in \mathbb{N}$ and fixed graph G on $\{1, 2, \ldots, n\}$.

As a consequence of our enumeration of Ω_n and (0.2) we shall prove in §3 the following.

Received 22 March 1988.

1980 *Mathematics Subject Classification* (1985 *Revision*) 11D09.

MAIN THEOREM. *For $n\in\mathbb{N}$, let $\lambda_n = \prod_{j=1}^{k}(1-2^{1-2j})$, where $k=[n/2]$. Then, for each fixed $n\in\mathbb{N}$,*

$$\liminf_{X\to\infty}\frac{\#\{d\in\mathscr{D}_n : d\leqslant X, (0.1)\text{ soluble}\}}{\#\{d\in\mathscr{D}_n : d\leqslant X\}} \geqslant \lambda_n. \tag{0.3}$$

We observe that λ_n converges to a limit $\lambda_\infty = 0.419422442\ldots$. It seems reasonable to conjecture that

$$\lim_{X\to\infty}\frac{\#\{d\in\mathscr{D} : d\leqslant X, (0.1)\text{ soluble}\}}{\#\{d\in\mathscr{D} : d\leqslant X\}} \geqslant \lambda_\infty, \tag{0.4}$$

but we are unable to prove this at present; our proof of (0.3) uses induction on n, and so cannot be adapted to attack (0.4).

REMARKS. 1. Our construction of $\gamma(d)$ is, in some ways, foreshadowed by certain devices used by Pumplün [**16**] and Trotter [**21**], although they do not employ graphs, and their results are contained as very special cases of our result (§1), that (0.1) is soluble if $\gamma(d)$ is odd. Pumplün's paper is mainly devoted to the study of the class-number h_d and narrow class-number h_d^* of the ring of integers $\mathcal{O}_d$ of $\mathbb{Q}(\sqrt{d})$. Our approach leads to a very simple proof of Pumplün's congruence [**16**, p. 195] for h_d^*, in the form

$$h_d^* \equiv 2^{n-1}\kappa_d \pmod{2^n}, \tag{0.5}$$

where κ_d is the number of spanning trees of $\gamma(d)$, and $d\in\mathscr{D}_n$. (See the Appendix for further references to related work on ideal class groups.)

2. A. G. Thomason (Cambridge) has enumerated Ω_n in a quite different context [**20**]; namely, he enumerates graphs G with no 'Eulerian bipartition'; that is, for no partition $\{1,2,\ldots,n\} = V_1\cup V_2$ into non-empty disjoint sets V_1, V_2 is the bipartite graph on V_1, V_2 induced by G an Eulerian graph. In §2 we show that such G are precisely the members of Ω_n. We are indebted to Dr Thomason for pointing this out to us during the preparation of this paper; after studying a preprint of [**20**] we have been able to produce an alternative, very simple enumeration of Ω_n which differs considerably from his. We are also indebted to Dr Thomason for supplying the reference [**17**] on 'bicycles', which we use in §2.

3. We clarify our earlier assertion about simple rational criteria for the solubility of (0.1). For any given $d\in\mathscr{D}_n$, we can decide the solubility of (0.1) by determining the parity of the period of the continued fraction expansion of $\sqrt{d}$ (see, for example, [**5**]). However, we cannot regard this as a simple rational criterion, since there is no way of predicting this parity *a priori* in terms (say) of congruence properties of d in $\mathbb{Z}$. After a long series of papers (see the references in [**16**]), L. Rédei obtained necessary and sufficient conditions for the solubility of (0.1), in terms of the class-fields of $\mathbb{Q}(\sqrt{d})$; again, we cannot regard these criteria as simple and rational, since there is no algorithm to test them which is simpler than checking (0.1) via the continued fraction expansion of $\sqrt{d}$; certainly Rédei's criteria are not reducible to congruences for d in $\mathbb{Z}$, since the relevant class-fields are not (in general) abelian over $\mathbb{Q}$.

4. Numerical evidence for $d\leqslant 10^6$ suggests that the criterion $\gamma(d)$ odd accounts for roughly 87 per cent of the d in $\mathscr{D}$ for which (0.1) is soluble. It would be interesting to have at least a heuristic explanation for this; perhaps a graph $\gamma^*(d)$ with 'coloured' edges, based on 2^kth-power residue symbols of the primes dividing d could be constructed, for $k=2,3,\ldots$, to produce further sufficient conditions for (0.1) to be soluble. We shall not pursue this question any further in this paper.

1. *The graph* $\gamma(d)$

First let $p, q \in \mathscr{D}_1$ as defined in §1; thus p, q are primes in $\mathbb{N}$, not congruent to 3 (mod 4). We define a relation $R \subset \mathscr{D}_1 \times \mathscr{D}_1$ via: $(p,q) \in R$ if and only if $p \neq q$ and p^3 is not congruent to a square modulo q^3. (Equivalently, $p \neq q$ and p is not a q-adic square.) By the quadratic reciprocity law [**5**], we see easily that R is symmetric, that is $(p,q) \in R$ if and only if $(q,p) \in R$.

For $d \in \mathscr{D}_n$ we factorise d into primes: $d = p_1 p_2 \dots p_n$, where $p_1 < p_2 < \dots < p_n$, and associate with d a graph on $\{1, 2, \dots, n\}$ as follows. Let $1 \leqslant i, j \leqslant n$. Then we join i to j with an edge if and only if $(p_i, p_j) \in R$; this process uniquely defines a graph, which we denote by $\gamma(d)$.

Now let $n \in \mathbb{N}$. We call a graph G on $\{1, 2, \dots, n\}$ *odd* if it has the following property. Whenever $\{1, 2, \dots, n\} = A \cup B$ with $A, B \neq \varnothing = A \cap B$, either there exists $a \in A$ joined (in G) to an odd number of $b \in B$, or vice versa (interchanging A and B). (If $n = 1$ we regard the sole graph on $\{1\}$ as being odd.)

The following simple result is the basis of all our later work in this paper.

PROPOSITION 1.1. *Let* $n \in \mathbb{N}$, $d \in \mathscr{D}_n$, *and suppose that* $\gamma(d)$ *is odd. Then* (0.1) *is soluble.*

REMARKS. 1. Special cases of this result appear in somewhat different versions in [**21**, **16**, **2**], with proofs involving ideal theory in $\mathscr{O}_d$. We present a completely elementary proof, working entirely within $\mathbb{Z}$; we are grateful to Professor Cassels for pointing out to us a simplification of our original argument.

2. The case where $n = 1$ is classical; Legendre gave a proof based on the continued fraction expansion of $\sqrt{d}$; see also [**3**].

3. The condition that $\gamma(d)$ be odd is not necessary. For example, if $d = 145 = 5 \cdot 29 \in \mathscr{D}_2$ or $d = 6409 = 13 \cdot 17 \cdot 29 \in \mathscr{D}_3$, then $\gamma(d)$ is not odd but (0.1) is soluble.

Proof of Proposition 1.1. Let (x, y) be a solution of the positive Pell equation $x^2 - dy^2 = +1$ with $y > 0$ minimal. Then x is odd, since otherwise $dy^2 \equiv -1 \pmod 4$, which is impossible, and $(x-1)(x+1) = x^2 - 1 = dy^2$. Since $(x-1, x+1) = 2$ and d is square-free, this gives

$$x + 1 = 2fx_1^2, \qquad x - 1 = 2gy_1^2,$$

where $f, g, x_1, y_1 > 0$, $fg = d$ and $y = 2x_1 y_1$. Subtracting gives

$$1 = fx_1^2 - gy_1^2. \tag{1.1}$$

Now if $g = 1$ and $f = d$ we have a solution to (0.1) immediately: $y_1^2 - dx_1^2 = -1$. If $f = 1$ and $g = d$ we have a new solution $x_1^2 - dy_1^2 = +1$ to the positive Pell equation, with $0 < y_1 \leqslant \frac{1}{2}y < y$, contradiction.

Finally suppose that $f, g > 1$; we replace (1.1) by the weaker equation

$$\pm 1 = fx_1^2 - gy_1^2, \tag{1.1}*$$

and prove it insoluble. Write $d = p_1 p_2 \dots p_n$ with p_i prime and $p_1 < p_2 < \dots < p_n$. Let

$$A = \{i : 1 \leqslant i \leqslant n, p_i | f\} \quad \text{and} \quad B = \{1, 2, \dots, n\} \setminus A = \{i : 1 \leqslant i \leqslant n, p_i | g\}.$$

Then, by assumption, $A \cap B = \varnothing \neq A, B$. Since $\gamma(d)$ is odd, either there is $a \in A$ joined to an odd number of $b \in B$ or vice versa. By symmetry, we may assume that some

$i \in A$ is joined to an odd number of $j \in B$. Then $(p_i, p_j) \in R$ for an odd number of $j \in B$. If $p = p_i \neq 2$ we see that the Legendre symbol $(g/p) = -1$, which contradicts (1.1)*, since $p \equiv 1 \pmod 4$. If $p = 2$, an odd number of prime factors of g are congruent to $5 \pmod 8$, while the remainder (if any) are congruent to $1 \pmod 8$. Hence $g \equiv 5 \pmod 8$, while $f \equiv 2 \pmod 8$. Hence, reducing (1.1)* modulo 8, we have

$$\pm 1 = 5y_1^2 - 2x_1^2 \pmod 8.$$

But then y_1 is odd, so $y_1^2 \equiv 1 \pmod 8$, and we have $5 \pm 1 \equiv 2x_1^2 \pmod 8$, which is impossible. Thus we see that (1.1) is impossible with $f > 1$ and $g > 1$, and the proposition is proved.

REMARK. Let $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$, let ε_0 be a fundamental unit of $\mathcal{O}_d$, and let ε be a fundamental unit of the subring $\mathbb{Z}[\sqrt{d}]$. Then it is easily checked that ε is either $\pm\varepsilon_0^{\pm 1}$ or $\pm\varepsilon_0^{\pm 3}$. Hence if $\gamma(d)$ is odd we have $N\varepsilon_0 = -1$, and so $h_d^* = h_d$, where h_d (respectively h_d^*) is the ordinary (respectively narrow) ideal class number of $\mathcal{O}_d$.

2. *Enumeration of odd graphs*

Let $n \in \mathbb{N}$ and set $\mathbf{n} = \{1, 2, \ldots, n\}$. We denote by $\mathcal{G}_n$ the set of all graphs on $\mathbf{n}$ as vertex set, and by Ω_n the set of odd graphs in $\mathcal{G}_n$. Then $\#\mathcal{G}_n = 2^{\binom{n}{2}}$ since there are $\binom{n}{2}$ possible edges for a graph on n vertices. In this section we shall enumerate Ω_n by seeking alternative characterisations of graphs in Ω_n.

Let V be the $\mathbf{F}_2$-vector space with $\mathbf{n}$ as basis, so that $V \cong \mathbf{F}_2^n$ (here $\mathbf{F}_2$ is the field of 2 elements). We may identify V with the space of subsets of $\mathbf{n}$ (with symmetric difference as addition) in an obvious way. Let $\mathbf{c} = (1, 1, \ldots, 1)^t \in \mathbf{F}_2^n$ (where ^{t} denotes transpose), so that $\mathbf{c}$ corresponds to the whole of $\mathbf{n}$ under the above identification. If $\mathbf{x} \in V$ then $\mathbf{x} + \mathbf{c}$ and $\mathbf{x}$ correspond to complementary subsets of $\mathbf{n}$. Thus the *bipartitions* $\not{p}$ of $\mathbf{n}$ (that is, the partitions of $\mathbf{n}$ into two disjoint parts) correspond bijectively to unordered pairs $\{\mathbf{x}, \mathbf{x} + \mathbf{c}\}$, hence to cosets of the subspace $\langle \mathbf{c} \rangle$ of V. We may therefore define the *bipartition space* $\mathcal{P}$ of $\mathbf{n}$ to be $\mathcal{P} = V/\langle \mathbf{c} \rangle$.

For each bipartition $\not{p} \in \mathcal{P}$ and for each graph $G \in \mathcal{G}_n$ we obtain an induced *bipartite graph* $G_{\not{p}}$ by deleting all the edges of G which join vertices in the same subpart. If every vertex in $\mathbf{n}$ has even degree in $G_{\not{p}}$ then $G_{\not{p}}$ is *Eulerian* (since each connected component of $G_{\not{p}}$ then has an Eulerian circuit in the sense of [**10**]). A graph G is *odd* if for each non-trivial bipartition $\not{p}$ of $\mathbf{n}$ the induced bipartite graph $G_{\not{p}}$ is *not* Eulerian; otherwise G is even. To enumerate the odd graphs we shall prove that for each $G \in \mathcal{G}_n$, the set of bipartitions $\not{p}$ for which $G_{\not{p}}$ is Eulerian forms an $\mathbf{F}_2$-subspace of $\mathcal{P}$, which is the kernel of a certain linear map $\mathbf{M}$ whose rank may be computed easily.

To define this map we use the incidence matrix of G. Let $e_1, e_2, \ldots, e_k$ be the edges of G; the *edge-space* E of G is the $\mathbf{F}_2$-vector space with $e_1, e_2, \ldots, e_k$ as basis, so that $E \cong \mathbf{F}_2^k$. The *incidence matrix* of G is the $n \times k$ matrix $\mathbf{A} = (a_{ij})$ with $a_{ij} = 1$ if $i \in e_j$ and $a_{ij} = 0$ otherwise. (Thus, each column of $\mathbf{A}$ has exactly two entries equal to 1.) We write $\mathbf{M} = \mathbf{A}\mathbf{A}^t$. The matrix-tree theorem [**10**] states that every $(n-1) \times (n-1)$ cofactor of $\mathbf{M}$ is equal to the number of spanning trees in G. We shall use the modulo 2 version of this theorem: interpreting $\mathbf{A}$ and $\mathbf{M}$ as matrices over $\mathbf{F}_2$, it says that G has an odd number of spanning trees if and only if $\operatorname{rank}(\mathbf{M}) = n-1$ (otherwise $\operatorname{rank}(\mathbf{M}) \leqslant n-2$). It will turn out that this condition is equivalent to G being odd.

An element $\mathbf{x}$ of E (that is, a subset of the edges of G) is a *cycle* if $\mathbf{Ax} = \mathbf{0}$, so that every vertex is incident with an even number of the edges in $\mathbf{x}$.

Since $\mathbf{A}$ is $n \times k$, the transpose $\mathbf{A}^t$ induces a linear map from $V \cong \mathbf{F}_2^n$ to $E \cong \mathbf{F}_2^k$. An element $\mathbf{x} \in E$ is a *cocycle* if $\mathbf{x} = \mathbf{A}^t\mathbf{y}$ for some $\mathbf{y} \in V$. Note that $\mathbf{A}^t\mathbf{c} = \mathbf{0}$, so that $\mathbf{A}^t\mathbf{y} = \mathbf{A}^t(\mathbf{y}+\mathbf{c})$, and hence $\mathbf{A}^t$ actually yields an $\mathbf{F}_2$-linear map from the bipartition space $\mathscr{P}$ to E: it assigns to each bipartition $\not{p}$ the set of edges which join vertices in 'opposite parts' of $\not{p}$. This is precisely the set of edges of the induced bipartite graph $G_{\not{p}}$.

LEMMA 2.1. *Let $\mathbf{y} \in V$ represent a bipartition $\not{p}$ in $\mathscr{P} = V/\langle \mathbf{c} \rangle$. Then $G_{\not{p}}$ is Eulerian if and only if $\mathbf{AA}^t\mathbf{y} = \mathbf{0}$.*

Proof. Let $\mathbf{x} = \mathbf{A}^t\mathbf{y}$, so that $\mathbf{x}$ is the set of edges in $G_{\not{p}}$. Then $G_{\not{p}}$ is Eulerian if and only if every vertex has even degree, that is, if and only if $\mathbf{Ax} = \mathbf{0}$.

The edge-set $\mathbf{x} = \mathbf{A}^t\mathbf{y}$ in this proof is thus both a cycle and a cocycle (when $G_{\not{p}}$ is Eulerian). Such objects are called *bicycles* (see [17]). A bicycle $\mathbf{x}$ is *non-trivial* if $\mathbf{Ax} = \mathbf{0}$ but $\mathbf{x} = \mathbf{A}^t\mathbf{y}$ for some $\mathbf{y} \neq \mathbf{0}, \mathbf{c}$.

We can now state our main result characterising odd graphs.

PROPOSITION 2.2. *Let $n \in \mathbb{N}$ and $G \in \mathscr{G}_n$. Then the following are equivalent.*

(1) *G is odd.*

(2) *For all non-zero $\not{p} \in \mathscr{P}$, the induced bipartite graph $G_{\not{p}}$ is not Eulerian.*

(3) *G has no non-trivial bicycles.*

(4) *G has an odd number of spanning trees.*

Proof. The equivalence of (1) and (2) is immediate from the definitions, while that of (2) and (3) follows directly from Lemma 2.1 and the definition of a bicycle.

We shall now show that (3) and (4) are equivalent. Let $\mathbf{M} = \mathbf{AA}^t$ as above. Then $\ker(\mathbf{M}) \supseteq \langle \mathbf{c} \rangle$, and we have

$$\begin{aligned} G \text{ has a non-trivial bicycle} &\Leftrightarrow \mathbf{M} \supset \langle \mathbf{c} \rangle \qquad \text{(strict inclusion)} \\ &\Leftrightarrow \dim(\ker(\mathbf{M})) \geqslant 2 \\ &\Leftrightarrow \operatorname{rank}(\mathbf{M}) \leqslant n-2 \\ &\Leftrightarrow G \text{ has an odd number of spanning trees,} \end{aligned}$$

the last step following from the matrix-tree theorem.

REMARK. The equivalence of (3) and (4) is due to Chen: see [17].

Using the equivalence of (1) and (4) in Proposition 2.2 we can now enumerate Ω_n. The first step reduces the problem to counting a certain set of matrices over $\mathbf{F}_2$.

LEMMA 2.3. *The following sets have the same cardinality, for each $n \in \mathbb{N}$:*

(1) Ω_n;

(2) *the set of all $n \times n$ symmetric matrices $\mathbf{M}$ over $\mathbf{F}_2$ with $\mathbf{Mc} = \mathbf{0}$ and $\operatorname{rank}(\mathbf{M}) = n-1$;*

(3) *the set of all non-singular $(n-1) \times (n-1)$ symmetric matrices over $\mathbf{F}_2$.*

Proof. $\#(1) = \#(2)$ For each $G \in \Omega_n$ the matrix $\mathbf{M} = \mathbf{A}\mathbf{A}^t$ is in set (2), by Proposition 2.2; conversely, each $\mathbf{M}$ in set (2) uniquely determines some $G \in \Omega_n$, by taking the off-diagonal part of $\mathbf{M}$ to be the adjacency matrix of G.

$\#(2) = \#(3)$ If $\mathbf{M}$ is in set (2) then every $(n-1) \times (n-1)$ minor of $\mathbf{M}$ has rank $n-1$; letting $\mathbf{M}_0$ be the (n,n) minor of $\mathbf{M}$ we see that $\mathbf{M}_0$ is in set (3). Conversely, given $\mathbf{M}_0$ in set (3), we can uniquely construct some $\mathbf{M}$ in set (2) with $\mathbf{M}_0$ as its (n,n) minor, since the entries in the nth row and column of $\mathbf{M}$ can clearly be chosen in exactly one way to make all the rows and columns of $\mathbf{M}$ sum to zero.

It follows that $\#\Omega_n = \sigma_{n-1}$, where σ_n is the number of non-singular symmetric $n \times n$ matrices over $\mathbf{F}_2$. We present here a simple method for calculating $\sigma_n = \sigma_n(q)$ which works for every finite field $\mathbf{F}_q$. An alternative method can be found in [12], using induction on n.

PROPOSITION 2.4. *Let q be a prime power, let $n \in \mathbb{N}$, and let $\sigma_n(q)$ be the number of non-singular $n \times n$ symmetric matrices over $\mathbf{F}_q$. Then*

$$\sigma_n(q) = q^{\binom{n+1}{2}} \prod_{0 < 2j \leqslant n+1} (1 - q^{1-2j}).$$

Proof. Let $V = \mathbf{F}_q^n$. There is an obvious bijection between the symmetric bilinear forms on V and the symmetric $n \times n$ matrices over $\mathbf{F}_q$. Each such form B is uniquely determined by its radical W, a subspace of V, and by a non-singular symmetric bilinear form on the quotient V/W. The total number of $n \times n$ symmetric matrices over $\mathbf{F}_q$ is clearly $q^{\binom{n+1}{2}}$. Hence we obtain the relation

$$q^{\binom{n+1}{2}} = \sum_{W \leqslant V} \sigma_{n-\dim W}(q) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q \sigma_{n-k}(q).$$

Here

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = H_q(n)/H_q(k)\,H_q(n-k),$$

where $H_q(k) = \prod_{i=1}^{k}(1-q^i)$ and $H_q(0) = 1$, so that $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the number of k-dimensional subspaces of $\mathbf{F}_q^n$. By using the obvious symmetry $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$ the previous equation can be simplified to

$$q^{\binom{n+1}{2}} = \sum_{k=0}^{n} \sigma_k(q) \frac{H_q(n)}{H_q(k)\,H_q(n-k)}. \tag{2.1}$$

Now let z be an indeterminate. We multiply (2.1) by $z^n/H_q(n)$, and sum over all $n \geqslant 0$, obtaining the following relation between formal power series over $\mathbb{Q}$:

$$\sum_{n \geqslant 0} z^n q^{\binom{n+1}{2}} H_q(n)^{-1} = \left(\sum_{k \geqslant 0} \sigma_k(q)\, z^k H_q(k)^{-1} \right) \left(\sum_{n \geqslant 0} z^n H_q(n)^{-1} \right). \tag{2.2}$$

Now it is clear by induction on n applied to (2.1) that there are polynomials $S_k(x) \in \mathbb{Z}[x]$, such that $\sigma_k(q) = S_k(q)$ for each prime power q and each $k \geqslant 0$. Hence, in (2.2), we may treat q as another indeterminate, and we may regard (2.2) as an identity in the ring $\mathbb{Q}[[z,q]]$ of formal power series in 2 variables z, q over $\mathbb{Q}$. This

ring R is complete in the $\mathcal{M}$-adic topology, where $\mathcal{M}$ is the maximal ideal $zR+qR$. We invoke the miraculous (but elementary) identities of Euler (see [**1**, p. 167]):

$$\prod_{n\geqslant 0}(1+q^n z)=\sum_{n\geqslant 0}q^{\binom{n}{2}}z^n H_q(n)^{-1} \tag{2.3a}$$

and

$$\prod_{n\geqslant 0}(1-zq^n)^{-1}=\sum_{n\geqslant 0}z^n H_q(n)^{-1} \tag{2.3b}$$

(where the infinite products are defined as $\prod_0^\infty = \mathcal{M}\text{-}\lim_{k\to\infty}\prod_0^k$).

Applying (2.3) repeatedly to (2.2), we have

$$\begin{aligned}\sum_{k\geqslant 0}\sigma_k(q)z^k H_q(k)^{-1} &= (1-z)\prod_{n\geqslant 0}(1+q^{2n}(-q^2z^2))\\ &= (1-z)\sum_{n\geqslant 0}(-1)^n q^{2n}z^{2n}q^{n(n-1)}/H_{q^2}(n).\end{aligned} \tag{2.4}$$

By comparing coefficients of z^m on each side of (2.4) we have

$$\sigma_m(q)=q^{\binom{m+1}{2}}\prod_{0<2j\leqslant m+1}(1-q^{1-2j}). \tag{2.5}$$

PROPOSITION 2.5. *Let $n\in\mathbb{N}$. Then*

$$\#\Omega_n = 2^{\binom{n}{2}}\prod_{0<2j\leqslant n}(1-2^{1-2j}).$$

Proof. This is immediate from Lemma 2.3 and Proposition 2.4.

REMARK. The above analysis can be modified to calculate the number of non-singular $n\times n$ symplectic matrices over $\mathbf{F}_q$. Redefining $\sigma_n(q)$ to be this number, we only need to replace $q^{\binom{n+1}{2}}$ by $q^{\binom{n}{2}}$ in (2.1) and imitate the above analysis. We leave the details to the reader.

3. *The distribution of $\gamma(d)$ as d varies*

As before, for $n\in\mathbb{N}$ let $\mathcal{G}_n$ be the set of all (labelled) graphs on $\{1,2,\ldots,n\}$. For $G\in\mathcal{G}_n$ we write $\mathcal{D}_n(G)=\{d\in\mathcal{D}_n:\gamma(d)=G\}$. For each fixed $n\in\mathbb{N}$ and $G\in\mathcal{G}_n$, we consider the asymptotic behaviour as $X\to\infty$ of

$$D_n(G,X):=\#\{d\in\mathcal{D}_n(G):d\leqslant X\}. \tag{3.1}$$

By induction on n we shall prove that

$$D_n(G,X)\sim 2^{-\binom{n}{2}}D_n(X), \tag{3.2}$$

where $D_n(X)=\#\{d\in\mathcal{D}_n:d\leqslant X\}$.

REMARKS. 1. Once (3.2) is proved, our main theorem (equation 0.3) follows immediately, in view of Proposition 2.5.

2. We observe that the asymptotic result

$$D_n(X)\sim c_n X(\log X)^{-1}(\log\log X)^{n-1}, \tag{3.3}$$

where $c_n=1/((n-1)!2^n)$, can be obtained by an easy modification of an old result of P. Turán and A. Selberg: see, for example, [**8**, p. 302].

3. The case in which $n=1$ of (3.2) is trivial since $\#\mathcal{G}_n=1$.

We now indicate how we may obtain (3.2) by induction. We assume that it has been proved for some n, take $G \in \mathscr{G}_{n+1}$, and consider $\mathscr{D}_{n+1}(G)$. When $k \in \mathbb{N}$ and $k > 1$, let $\tilde{k}$ be the largest prime divisor of k. Then there is a unique $H \in \mathscr{G}_n$ such that $d/\tilde{d} \in \mathscr{D}_n(H)$ for all $d \in \mathscr{D}_{n+1}(G)$. Conversely, let $t \in \mathscr{D}_n(H)$. Then for such t there is a unique corresponding set A_t of invertible residue classes (modulo $4t$) such that $d = pt \in \mathscr{D}_{n+1}(G)$ and $d/\tilde{d} = t$ if and only if p is a prime, $p > \tilde{t}$, and p belongs to A_t. This argument immediately gives

$$D_{n+1}(G, X) = \sum_{t \in T} \#\{\text{primes } p : \tilde{t} < p \leqslant Xt^{-1}, p \in A_t\}, \tag{3.5}$$

where $T = \mathscr{D}_n(H)$. For convenience we write $T(X) = \#\mathscr{D}_n(H, X)$. Then we wish to show that

$$D_{n+1}(G, X) \sim 2^{-\binom{n+1}{2}} D_{n+1}(X) \sim n^{-1} 2^{-1-n} T(X) (\log\log X), \tag{3.6}$$

given that

$$T(X) \sim 2^{-\binom{n}{2}} D_n(X), \tag{3.7}$$

and we shall do this by exploiting (3.5). It is convenient when $A \subseteq \mathbb{N}$ to write $\sum_{t \in A}^{*} f(t)$ in place of $\sum_{t \in T \cap A} f(t)$.

The proof of (3.6) is considerably simplified by using the following result.

LEMMA 3.1. *Let $M \geqslant 20$, $M < N \leqslant X^{n/(n+1)}$, and let*

$$\mathrm{Li}(y) = \int_2^y \frac{du}{\log u} \quad \text{for } y \geqslant 2.$$

Then

$$\sum_{M < t \leqslant N}^{*} \mathrm{Li}(Xt^{-1}) = o(D_{n+1}(X)) \tag{3.8}$$

if either

(i) $M = 20$ *and* $N = (\log X)^{100}$, *or*
(ii) $M = \exp[(\log X)/(\log\log X)^{100}]$ *and* $N = X^{n/(n+1)}$.

Moreover,

$$\sum_{M < t \leqslant N}^{*} \mathrm{Li}(Xt^{-1}) \sim n^{-1} T(X) \log\log X \tag{3.9}$$

if

$$M = (\log X)^{100} \quad \text{and} \quad N = \exp\left(\frac{\log X}{(\log\log X)^{100}}\right).$$

Proof. We begin by transforming $\sum_{M < t \leqslant N}^{*} \mathrm{Li}(Xt^{-1})$ by summation-by-parts. We have

$$\begin{aligned}\sum_{M < t \leqslant N}^{*} \mathrm{Li}(Xt^{-1}) &= \sum_{M < k \leqslant N} \mathrm{Li}(Xk^{-1})\{T(k) - T(k-1)\} \\ &= \sum_{k=M}^{N} \{\mathrm{Li}(Xk^{-1}) - \mathrm{Li}(X(k+1)^{-1})\} T(k) \\ &\quad + T(N)\,\mathrm{Li}(X(N+1)^{-1}) - T(M)\,\mathrm{Li}(XM^{-1}).\end{aligned}$$

Now

$$T(M)\,\mathrm{Li}(XM^{-1}) = O(D_n(M)\,\mathrm{Li}(XM^{-1})) = O\left(\frac{X}{\log X}\frac{(\log\log M)^{n-1}}{\log M}\right) = o(D_{n+1}(X)),$$

and similarly

$$T(N)\,\mathrm{Li}(X(N+1)^{-1}) = o(D_{n+1}(X)),$$

for the various choices of M, N in the statement of the lemma. Thus it suffices to handle the asymptotics of

$$\sum_{k=M}^{N} T(k)\{\mathrm{Li}\,(Xk^{-1}) - \mathrm{Li}\,(X(k+1)^{-1})\}.$$

By the mean-value theorem,

$$\mathrm{Li}(Xk^{-1}) - \mathrm{Li}\,(X(k+1)^{-1}) = \frac{X}{k(k+1)}(\log X(k+\theta_k)^{-1})^{-1}$$

for some $0 < \theta_k < 1$. Thus

$$\sum_{k=M}^{N} (\mathrm{Li}\,(Xk^{-1}) - \mathrm{Li}(X(k+1)^{-1}))\,T(k) = X \sum_{k=M}^{N} T(k) \Big/ \left\{k(k+1)\log\frac{X}{k+\theta_k}\right\}. \quad (3.10)$$

First, if $M = 20$ and $N = (\log X)^{100}$, we see that the right-hand side of (3.10) is

$$\begin{aligned}\frac{X(1+O(1))}{\log X}\sum_{k=M}^{N}\frac{T(k)}{k(k+1)} &= \frac{X}{\log X}(1+O(1))\left\{\int_M^{N+1}\frac{T(k)\,dk}{k^2} + o(1)\right\}\\ &= O\left(\frac{X}{\log X}\int_M^{N+1}\frac{(\log\log k)^{n-1}dk}{k\log k}\right)\\ &= O\left(\frac{X}{\log X}(\log\log\log X)^n\right)\\ &= o(D_{n+1}(X)).\end{aligned}$$

Secondly, if

$$M = \exp\left\{\frac{\log X}{(\log\log X)^{100}}\right\} \quad \text{and} \quad N = X^{n/(n+1)},$$

then the right-hand side of (3.10) is

$$\begin{aligned}O\left(\frac{X}{\log X}\int_M^N\frac{T(k)\,dk}{k^2}\right) &= O\left(\frac{X}{\log X}\{(\log\log N)^n - (\log\log M)^n\}\right)\\ &= O\left(\frac{X}{\log X}(\log\log N)^{n-1}\log\left(\frac{\log N}{\log M}\right)\right)\\ &= o(D_{n+1}(X)).\end{aligned}$$

Finally, if

$$M = (\log X)^{100} \quad \text{and} \quad N = \exp\left\{\frac{\log X}{(\log\log X)^{100}}\right\},$$

the right-hand side of (3.10) is

$$(1+o(1))\frac{X}{\log X}\int_M^N\frac{T(k)\,dk}{k^2} = (1+o(1))\,n^{-1}T(X)\log\log X,$$

since $\log\log N \sim \log\log X$ and $\log\log M = O(\log\log\log X)$. This proves the lemma.

We now return to (3.5). We first observe that if $t \in T = \mathscr{D}_n(H)$ and $t > X^{n/(n+1)}$ then $\tilde{t} > X^{1/(n+1)}$, $\tilde{t} > X/t$, and so such t make no contribution to (3.5). For our first

reduction we subdivide the right-hand side of (3.5) into the contribution E_1 made by the $t \in T$ with

$$\mu = \exp\left\{\frac{\log X}{(\log\log X)^{100}}\right\} < t \leqslant X^{n/(n+1)},$$

and the contribution F_1 made by the $t \in T$ for which $1 < t \leqslant \mu$. We show that E_1 is negligible; for this, we use the trivial inequality

$$0 \leqslant \#\{\text{primes } p : \tilde{t} < p \leqslant Xt^{-1}, p \in A_t\} \leqslant \pi(Xt^{-1}) = O(\mathrm{Li}(Xt^{-1})),$$

where $\pi(y) = \#\{\text{primes } p \leqslant y\}$. Summing over the $t \in T$ with $\mu < t \leqslant X^{n/(n+1)}$, we see that $E_1 = o(D_{n+1}(X))$, by using (3.8)(ii).

Next we decompose F_1 into $F_2 + E_2$, where E_2 is the contribution of the $t \in T$ with $t \leqslant \lambda = (\log X)^{100}$. The $t \leqslant 20$ contribute $O(X/\log X)$, while the $t \in T$ with $20 < t \leqslant \lambda$ contribute (arguing as for E_1) an amount which is $o(D_{n+1}(X))$, by (3.8)(i). This gives $E_2 = o(D_{n+1}(X))$, and we now have

$$D_{n+1}(G, X) = \sum_{\lambda < t \leqslant \mu}^{*} \#\{\text{primes } p : \tilde{t} < p \leqslant Xt^{-1}, p \in A_t\} + o(D_{n+1}(X)). \tag{3.11}$$

Since for $\lambda < t \leqslant \mu$ we have $\tilde{t} < Xt^{-1}$, we thus have

$$D_{n+1}(G, X) = \sum_{\lambda < t \leqslant \mu}^{*} \{\pi(Xt^{-1}, A_t, 4t) - \pi(\tilde{t}, A_t, 4t)\} + o(D_{n+1}(X)), \tag{3.12}$$

where $\pi(y, B, q)$ is the number of primes $p \leqslant y$ such that $p \in B \pmod q$. Now the contribution of the terms $\pi(\tilde{t}, A_t, 4t)$ to (3.12) is at most

$$O\left(\sum_{\lambda < t \leqslant \mu}^{*} \pi(t)\right) = O(\mu\pi(\mu)) = O\left(\frac{\mu^2}{\log \mu}\right),$$

which is clearly $o(D_{n+1}(X))$. Hence we have

$$D_{n+1}(G, X) = \sum_{\lambda < t \leqslant \mu}^{*} \pi(Xt^{-1}, A_t, 4t) + o(D_{n+1}(X)). \tag{3.13}$$

We must show that

$$V = \sum_{\lambda < t \leqslant \mu}^{*} \pi(Xt^{-1}, A_t, 4t) \sim n^{-1}2^{-n-1}T(X)\log\log X,$$

and this requires some rather delicate arguments involving the error term in the prime number theorem for arithmetic progressions. The proof is hindered by the possible existence of exceptional ('Siegel'-) zeros of the corresponding L-functions, and we need to divide the $t \in T$ in $(\lambda, \mu]$ into two types. First, those for which none of the relevant L-functions has a real zero 'close' to $s = 1$, in which case we have a good asymptotic approximation for $\pi(Xt^{-1}, A_t, 4t)$; and secondly, those where some relevant L-function has such a zero, in which case we can only use the trivial upper bound $O(\pi(Xt^{-1}))$ for $\pi(Xt^{-1}, A_t, 4t)$. Roughly speaking, the t of the second type are sufficiently rare that (in the end) they are seen to make a negligible contribution to V.

The following simple but crucial observation makes this programme feasible. In deciding when $k \in \mathbb{Z}$ is in A_t (modulo $4t$) we only need to use the real Dirichlet characters arising from the relevant quadratic characters whose conductors q are the odd primes dividing t (together with $q = 8$ if t is even). These generate a subgroup Γ_t of order 2^{n+1} in the character group of $(\mathbb{Z}/4t\mathbb{Z})^*$, and it is clear that $\#\Gamma_t \cdot \# A_t = \phi(4t)$, so that $\# A_t = \phi(4t)/2^{n+1}$, where ϕ is Euler's function.

In order to prove that V above is asymptotic to $n^{-1}2^{-n-1}T(X)\log\log X$, it is sufficient, and much more convenient, to apply the standard asymptotic relations [**6**, p. 112] connecting $\psi(x,B,q)$ with $\pi(x,B,q)$, and then to prove that

$$\sum_{\lambda<t\leqslant\mu}^{*}\psi(Xt^{-1},A_t,4t)\sim n^{-1}2^{-n-1}T(X)\log\log X\log X. \tag{3.14}$$

Here, as usual, we have

$$\psi(y,B,q)=\sum_{\substack{m\leqslant y\\ m\in B\,(\mathrm{mod}\,q)}}\Lambda(m)\quad\text{and}\quad\Lambda(m)=\begin{cases}\log p & \text{if } m=p^k, p \text{ prime}, k\geqslant 1,\\ 0 & \text{otherwise.}\end{cases} \tag{3.15}$$

If χ is a character modulo q, we put

$$\psi(y,\chi)=\sum_{m\leqslant y}\chi(m)\Lambda(m). \tag{3.16}$$

Then the orthogonality relations in Γ_t yield

$$\left|\psi(x,A_t,4t)-\frac{\psi(x,\chi_0)}{2^{n+1}}\right|\leqslant E_3, \tag{3.17}$$

where $E_3=\max\{|\psi(x,\chi)|:\chi\in\Gamma_t,\chi\neq\chi_0\}$, χ_0 is the principal character (modulo $4t$), and we put $x=Xt^{-1}$. By results of Page (see [**6**, §14 and §20]) there is an absolute constant $c_1>0$ such that $L(s,\chi)\neq 0$ for $s\geqslant 1-c_1/\log 4\mu$ for every non-principal real character of conductor $q\leqslant 4\mu$, with possibly one exceptional conductor q_1. By applying Siegel's theorem [**6**, §21] in place of the argument of [**6**, p. 124], we may assume that

$$q_1>(\log\mu)^{100}. \tag{3.18}$$

Now, by [**6**, p. 122], for every $\chi\neq\chi_0$ in Γ_t, we have

$$|\psi(x,\chi)|\leqslant 2x^{\beta(\chi)}+x\log^2 xt\left\{c_2\exp\left(-c_3\frac{\log x}{\log t}\right)+c_4t^{-4}\right\}+c_5x^{\frac{1}{4}}\log x \tag{3.19}$$

for certain absolute constants $c_2,\ldots,c_5>0$ and $X>X_0$. Here

$$\beta(\chi)=\max\{s\in\mathbb{R}:s\geqslant\tfrac{1}{2},L(s,\chi)=0\}, \tag{3.20}$$

and we have chosen $T=t^4$ in (4) and (6) of [**6**, p. 122]. Now let

$$\beta(t)=\max\{\beta(\chi):\chi\in\Gamma_t,\chi\neq\chi_0\}; \tag{3.21}$$

then we have

$$0\leqslant E_3\leqslant 2x^{\beta(t)}+x\log^2 xt\left\{c_2\exp\left(-c_3\frac{\log x}{\log t}\right)+c_4t^{-4}\right\}+c_5x^{\frac{1}{4}}\log x, \tag{3.22}$$

with E_3 as in (3.17).

Now let

$$R=\{t\in T:\lambda<t\leqslant\mu,t\not\equiv 0\,(\mathrm{mod}\,q_1)\}\quad\text{and}\quad S=\{t\in T:\lambda<t\leqslant\mu,t\equiv 0\,(\mathrm{mod}\,q_1)\},$$

with q_1 defined as in (3.18). Then, for $t\in R$, we have $\beta(t)\leqslant 1-c_1/\log 4\mu$. Hence, by (3.22), recalling that $x=Xt^{-1}$, we have

$$\begin{aligned}0\leqslant E_3\leqslant{}& 2Xt^{-1}\exp\left(-c_1\frac{\log Xt^{-1}}{\log 4\mu}\right)+c_2Xt^{-1}\log^2 X\exp\left(-c_3\frac{\log Xt^{-1}}{\log t}\right)\\ &+c_4Xt^{-5}\log^2 X+c_5(Xt^{-1})^{\frac{1}{4}}\log Xt^{-1}\end{aligned} \tag{3.23}$$

for all $t \in R$. Summing over all such t, we have

$$0 \leqslant \sum_{t \in R} E_3 \leqslant \mathscr{E}_1 + \mathscr{E}_2 + \mathscr{E}_3 + \mathscr{E}_4 \qquad (\mathscr{E}_i \geqslant 0). \tag{3.24}$$

We show that $\mathscr{E}_1, \ldots, \mathscr{E}_4$ are all $o(D_{n+1}(X)\log X)$.

We have

$$\begin{aligned}\mathscr{E}_1 &= O\left(X \sum_{t \in R} t^{-1} \exp\left(-\tfrac{1}{2}c_1 \frac{\log X}{\log \mu}\right)\right) \\ &= O\left(X \exp\left(-\tfrac{1}{2}c_1 \frac{\log X}{\log \mu}\right) \log \mu\right) \\ &= O\left(\frac{X \log X}{(\log\log X)^{100}} \exp\left(-\tfrac{1}{2}c_1 (\log\log X)^{100}\right)\right),\end{aligned}$$

which is clearly $o(D_{n+1}(X)\log X)$. The term $\mathscr{E}_2$ is estimated in the same way, with an additional factor $\log X$; it is still $o(D_{n+1}(X)\log X)$. Further we have

$$\begin{aligned}0 \leqslant \mathscr{E}_3 &\leqslant c_4 X \log^2 X \sum_{t \in R} t^{-5} = O(X \log^2 X \cdot \lambda^{-4}) \\ &= O(X \log^2 X (\log X)^{-400}) = o(D_{n+1}(X)\log X).\end{aligned}$$

Finally,

$$\begin{aligned}0 \leqslant \mathscr{E}_4 &\leqslant c_5 X^{\frac{1}{4}} \sum_{t \in R} t^{-\frac{1}{4}} \log X t^{-1} \leqslant c_5 X^{\frac{1}{4}} \log X \sum_{t \in R} t^{-\frac{1}{4}} \\ &= O(X^{\frac{1}{4}} \log X \cdot \mu^{\frac{3}{4}}) = o(X^{\frac{1}{2}}) = o(D_{n+1}(X)\log X).\end{aligned}$$

Combining these results, we have

$$\left| \sum_{t \in R} \left(\psi(Xt^{-1}, A_t, 4t) - \frac{1}{2^{n+1}} \psi(Xt^{-1}, \chi_0) \right) \right| = o(D_{n+1}(X)\log X),$$

that is,

$$\sum_{t \in R} \psi(Xt^{-1}, A_t, 4t) = \frac{1}{2^{n+1}} \sum_{t \in R} \psi(Xt^{-1}) + o(D_{n+1}(X)\log X). \tag{3.25}$$

To handle the t in S, we use

$$\begin{aligned}0 \leqslant \sum_{t \in S} \psi(Xt^{-1}, A_t, 4t) &\leqslant \sum_{t \in S} \psi(Xt^{-1}) = O\left(X \sum_{t \in S} t^{-1}\right) \\ &= O\left(\frac{X}{q_1} \sum_{m=1}^{\mu q_1^{-1}} m^{-1}\right) = O(X q_1^{-1} \log \mu),\end{aligned}$$

since the $t \in S$ are necessarily in $q_1 \mathbb{Z}$. By (3.18) we have

$$0 \leqslant \sum_{t \in S} \psi(Xt^{-1}, A_t, 4t) = O(X(\log \mu)^{-99}) = o(D_{n+1}(X)\log X). \tag{3.26}$$

Combining (3.25) and (3.26), we have

$$\sum_{\lambda < t \leqslant \mu}^{*} \psi(Xt^{-1}, A_t, 4t) = 2^{-n-1} \sum_{\lambda < t \leqslant \mu}^{*} \psi(Xt^{-1}) + o(D_{n+1}(X)\log X). \tag{3.27}$$

Finally we have

$$\begin{aligned}\sum_{\lambda < t \leqslant \mu}^{*} \psi(Xt^{-1}) &= \sum_{\lambda < t \leqslant \mu}^{*} (\log Xt^{-1}) \operatorname{Li}(Xt^{-1}) \{1 + o(1)\} \\ &= \log X (1 + o(1)) \sum_{\lambda < t \leqslant \mu}^{*} \operatorname{Li}(Xt^{-1}) \\ &\sim n^{-1} T(X) \log X \log\log X,\end{aligned}$$

by (3.9), and this, combined with (3.27), gives (3.14), and hence (3.6). Thus (3.2) is established with $n+1$ in place of n, and there is nothing more to prove.

References

1. G. E. ANDREWS, *Number theory* (W. B. Saunders Co., Philadelphia, 1971).
2. H. COHN, *A classical invitation to algebraic numbers and class-fields* (Springer, New York, 1978).
3. H. COHN, *Advanced number theory* (Dover, New York, 1980).
4. H. COHN and J. C. LAGARIAS, 'On the existence of fields governing the 2-invariants of the class group of $\mathbb{Q}(\sqrt{(dp)})$ as p varies', *Math. Comp.* 41 (1983) 711–730.
5. H. DAVENPORT, *The higher arithmetic* (Hutchinson, London, 1952).
6. H. DAVENPORT, *Multiplicative number theory*, 2nd edition (Springer, New York, 1980).
7. L. E. DICKSON, *History of the theory of numbers*, vol. II (Chelsea, New York, 1952).
8. P. D. T. A. ELLIOTT, *Probabilistic number theory* II (Springer, New York, 1980).
9. F. GERTH III, 'The 4-class ranks of quadratic fields', *Invent. Math.* 77 (1984) 489–515.
10. F. HARARY, *Graph theory* (Addison–Wesley, Reading, Mass., 1969).
11. J. C. LAGARIAS, 'On determining the 4-rank of the ideal class group of a quadratic field', *J. Number Theory* 12 (1980) 191–196.
12. J. MACWILLIAMS, 'Orthogonal matrices over finite fields', *Amer. Math. Monthly* 76 (1969) 152–164.
13. P. MORTON, 'On Rédei's theory of the Pell equation', *J. Reine Angew. Math.* 307/8 (1979) 373–398.
14. P. MORTON, 'Density results for 2-classgroups and fundamental units of real quadratic fields', *Studia Sci. Math. Hungar.* 17 (1982) 21–43.
15. W. NARKIEWICZ, *Elementary and analytic theory of algebraic numbers* (PWN, Warszawa, 1974).
16. D. PUMPLÜN, 'Über die Klassenzahl und die Grundeinheit des reell-quadratischen Zahlkörpers', *J. Reine Angew. Math.* 230 (1968) 167–210.
17. P. ROSENSTIEHL and R. C. READ, 'On the principal edge tripartition of a graph', *Ann. of Discrete Math.* 3 (1978) 195–226.
18. L. RÉDEI, 'Über die Pellsche Gleichung $t^2 - du^2 = -1$', *J. Reine Angew. Math.* 173 (1935) 193–211.
19. P. STEVENHAGEN, 'Classgroups and governing fields', Report 88-08, Department of Mathematics, University of Amsterdam 1988.
20. A. G. THOMASON, 'A graph property not satisfying a "zero-one" law', *European J. Combin.* 9 (1988) 517–522.
21. H. F. TROTTER, 'On the norms of units in quadratic fields', *Proc. Amer. Math. Soc.* 22 (1969) 198–201.

APPENDIX

On receiving a preprint of this paper, J. C. Lagarias (A.T.&T. Laboratories, Murray Hill) pointed out that our reformulation (0.5) of Pumplün's congruence for h_d^* appears in his paper [**11**]. In that paper Lagarias considers the 4-rank e_2 of the narrow ideal class group of a general quadratic field; for real quadratic fields $\mathbb{Q}(\sqrt{d})$, $d \in \mathcal{D}_n$, Lagarias shows that $e_2 = 0$ if and only if the graph $\gamma(d)$ is odd, but he does not enumerate odd graphs or consider density questions. In particular, the results in our paper, together with his, yield the asymptotic distribution of the $d \in \mathcal{D}_n$ with $e_2 = 0$ (and hence also of the $d \in \mathcal{D}_n$ with $e_2 > 0$). Lagarias has also supplied supplementary references to recent work by various authors concerned with the 2^i-ranks of narrow ideal class groups of quadratic fields [**4, 9, 11, 13, 14, 19**]. It seems probable that some of this recent work could be used to improve our lower bound for the density of $d \in \mathcal{D}_n$ for which the negative Pell equation is soluble, although it is not clear at present how to do this.

Department of Mathematics
University of Exeter
North Park Road
Exeter EX4 4QE