Proc. Roy. Soc. Lond. A. **322**, 405–420 (1971)
Printed in Great Britain

On the density of discriminants of cubic fields. II

BY H. DAVENPORT, F.R.S. AND H. HEILBRONN, F.R.S.†
† *Department of Mathematics, University of Toronto, Canada*

(*Received* 13 *August* 1970)

An asymptotic formula is proved for the number of cubic fields of discriminant $\mathfrak{d}$ in $0 < \mathfrak{d} < X$; and in $-X < \mathfrak{d} < 0$.

1. INTRODUCTION

Let $N_3(\xi, \eta)$ denote the number of cubic fields K with discriminant $\mathfrak{d}_K$ satisfying $\xi < \mathfrak{d}_K < \eta$, where a triplet of conjugate fields is counted once only. The main purpose of this paper is to prove

THEOREM 1.
$$X^{-1}N_3(0, X) \to (12\zeta(3))^{-1} \quad as \quad X \to \infty,$$
$$X^{-1}N_3(-X, 0) \to (4\zeta(3))^{-1} \quad as \quad X \to \infty.$$

In a previous paper (Davenport & Heilbronn 1969) we proved the weaker result that the upper and lower limits are finite and positive. This proof is a refinement of our previous method. We showed then that there exists a discriminant-preserving 1–1 relation between cubic fields and a subset U of the classes of irreducible primitive cubic binary forms $F(x, y)$ with coefficients in $\mathbf{Z}$. In this paper U will be determined explicitly by congruence conditions on the coefficients of F. Using an easy generalization of Davenport's earlier results on the class-number of binary cubic forms (Davenport 1951*a*, *b*) we obtain an estimate of the cardinality of U, and thus theorem 1.

As a by-product, two further results will be obtained. Let K_6 be the sextic normal extension of the non-cyclic cubic field K, and let p be a rational prime unramified in K (and hence in K_6). Then the Frobenius–Artin symbol $\{(K_6/Q)/p\}$ is defined as a conjugacy class of the S_3, its values being I or $A_3 - I$ or $S_3 - A_3$, where I is the identity class of S_3. Then it is a consequence of the Frobenius–Chebotarev density theorem that for fixed K and varying p (unramified in K) the values I, $A_3 - I$, $S_3 - A_3$ occur with relative frequency 1 : 2 : 3. We shall prove

THEOREM 2. *Let p be a fixed prime, and let K run through the cubic non-cyclic fields in which p does not ramify, the fields being ordered by the size of the discriminants. Then the Frobenius–Artin symbol $\{(K_6/Q)/p\}$ takes the values I, $A_3 - I$, $S_3 - A_3$ with relative frequency* 1 : 2 : 3.

Actually we shall do a little more. We shall also determine for each p the density of cubic fields K in which p is totally ramified, and the density of fields K in which p is partially ramified.

Another application of the method of this paper deals with the 3-class-number of quadratic fields. Let $h_3^*(\Delta_2)$ be the number of those ideal classes in the quadratic field of discriminant Δ_2 whose cube is the unit class. We shall prove

THEOREM 3. $$\sum_{0<\Delta_2<X} h_3^*(\Delta_2) \sim \tfrac{4}{3} \sum_{0<\Delta_2<X} 1 \quad as \quad X \to \infty,$$

$$\sum_{-X<\Delta_2<0} h_3^*(\Delta_2) \sim 2 \sum_{-X<\Delta_2<0} 1 \quad as \quad X \to \infty.$$

This theorem suggests the possibility that the relative density of positive and negative discriminants Δ_2 for which the congruence $h_3^*(\Delta_2) \equiv 0 (\mathrm{mod}\, 3^n)$ holds, is 3^{-2n} and 3^{1-2n} respectively for $n > 0$. But at the moment there does not seem to be any hope of proving results of this nature.

2. NOTATION AND DEFINITIONS

Small roman letters are reserved for rational integers, p is always a positive prime.

Φ is the set of all irreducible primitive binary cubic forms

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$$

of discriminant $$D = b^2c^2 + 18abcd - 27a^2d^2 - 4b^3d - 4c^3a.$$

The letters a, b, c, d and D will always be reserved for the coefficients and discriminant of the form F.

Two forms $F(x, y)$ and $F'(x', y')$ are called equivalent, or integrally equivalent, if there exists a unimodular 2 by 2 matrix M of determinant ± 1 such that the substitution $(x', y') = M(x, y)$ transforms F' into F. For quadratic forms we retain the classical definition of equivalence, which requires that $\det(M) = 1$.

Two forms $F(x,y)$ and $F'(x',y')$ in Φ are called rationally equivalent if there exists a non-singular 2 by 2 matrix M over $\mathbf{Z}$ such that the substitution $(x',y') = M(x,y)$ transforms F' into δF, where $\delta \neq 0$ is rational. This definition will only be used in § 6.

The congruence $F_1(x,y) \equiv F_2(x,y)\,(\mathrm{Mod}\, m)$ will denote that each coefficient of F_1 is congruent $(\mathrm{mod}\, m)$ to the corresponding coefficient of F_2, whereas

$$F_1(x,y) \equiv F_2(x,y)\,(\mathrm{mod}\, m)$$

will imply only that for each pair $x, y \in \mathbf{Z}$ the forms assume values congruent to each other $(\mathrm{mod}\, m)$.

Now we define the symbol (F,p) for $F \in \Phi$. We put

$$(F,p) = (111) \quad \text{if} \quad F \equiv \lambda_1(x,y)\lambda_2(x,y)\lambda_3(x,y) \quad (\mathrm{Mod}\, p),$$

where λ_1, λ_2, λ_3 are linear forms mod p, no two of which have a constant quotient.

$$(F,p) = (12) \quad \text{if} \quad F(x,y) \equiv \lambda(x,y)\,\kappa(x,y) \quad (\mathrm{Mod}\, p),$$

where $\lambda(x,y)$ is a linear form and $\kappa(x,y)$ is a quadratic form which is irreducible Mod p.

$$(F,p) = (3) \quad \text{if} \quad F(x,y) \equiv \kappa(x,y) \quad (\text{Mod}\, p),$$

where $\kappa(x,y)$ is irreducible Mod p.

$$(F,p) = (1^3) \quad \text{if} \quad F(x,y) \equiv \alpha\lambda^3(x,y) \quad (\text{Mod}\, p),$$

where $\lambda(x,y)$ is a linear form, and α a constant mod p.

$$(F,p) = (1^2\,1) \quad \text{if} \quad F(x,y) \equiv \lambda_1^2(x,y)\,\lambda_2(x,y) \quad (\text{Mod}\, p),$$

where $\lambda_1(x,y)$ and $\lambda_2(x,y)$ are linear forms with a non-constant quotient.

If F_1 and F_2 are either equivalent or congruent (Mod p) clearly $(F_1,p) = (F_2,p)$. Note also that $p|D$ if and only if $(F,p) = (1^3)$ or $(F,p) = (1^2\,1)$; further that $(F,p) = (1^3)$ implies $p^2|D$. By $T_p(111)$, $T_p(12)$, etc., we denote the set of $F \in \Phi$ for which $(F,p) = (111)$, $(F,p) = (12)$, etc. (Clearly each set T_p consists of classes of equivalent forms.) We define W_p by the relation

$$F \in W_p \Leftrightarrow D \equiv 0 \pmod{p^2}.$$

Next we define for each p subsets V_p and U_p of Φ. $F \in V_2$ if $D \equiv 1 \pmod 4$ or if $D \equiv 8$ or $12 \pmod{16}$. $F \in V_p$ for $p \neq 2$ if $F \notin W_p$. $F \in U_p$ if $F \in V_p$ or if $(F,p) = (1^3)$ and if the congruence $F(x,y) \equiv ep \pmod{p^2}$ has a solution for some $e \not\equiv 0 \pmod p$. Finally we put

$$V = \bigcap_p V_p, \quad U = \bigcap_p U_p.$$

Clearly all the sets V_p, U_p, V and U consist of complete classes of equivalent forms.

By the letter K we denote a cubic number field, by $\mathfrak{d}_K$ the discriminant of K. If $\alpha \in K$, we denote by $\mathrm{Nm}(\alpha)$, $\mathrm{tr}(\alpha)$, $\mathfrak{d}(\alpha)$ the norm, trace and discriminant of α taken in K over $\boldsymbol{Q}$.

Let S be a subset of Φ consisting of complete equivalence classes. Then we denote by $N(\xi,\eta;S)$ the number of classes in S whose forms have a discriminant D with $\xi < D < \eta$.

Let $\Delta_2 \in \boldsymbol{Z}$, $\Delta_2 \equiv 0$ or $1 \pmod 4$, Δ_2 not a square. Then $h_3^*(\Delta_2)$ denotes the number of those classes of primitive quadratic form of discriminant Δ_2 whose cube is the unit class. If Δ_2 is a field discriminant, this definition agrees with the definition given in the introduction.

$\tau(n)$ denotes the number of positive divisors of n.

Constants implied in the symbol O are independent of all parameters.

3. Local densities

In this section we consider forms $F \in \Phi$ over the residue class ring mod p^r for $r = 1$ and $r = 2$. Naturally, we neglect irreducibility over $\boldsymbol{Q}$. The number of such forms is $p^{4r}(1-p^{-4})$. Let S be a set of forms in Φ. We denote by $A(S;p^r)$ the number of residue classes mod p^r occupied by forms in S, divided by $p^{4r}(1-p^{-4})$.

Lemma 1. *For $r = 1$ and $r = 2$*

$$A(T_p(111); p^r) = \tfrac{1}{6}p(p-1)(p^2+1)^{-1},$$
$$A(T_p(12); p^r) = \tfrac{1}{2}p(p-1)(p^2+1)^{-1},$$
$$A(T_p(3); p^r) = \tfrac{1}{3}p(p-1)(p^2+1)^{-1},$$
$$A(T_p(1^3); p^r) = (p^2+1)^{-1},$$
$$A(T_p(1^2 1); p^r) = p(p^2+1)^{-1}.$$

Proof. As the definition of (F,p) depends only on the residue-class of $F\,(\mathrm{Mod}\,p)$, it suffices to prove the lemma for $r = 1$. Call a form normalized if the highest non-vanishing coefficient equals 1. It is well known that the number of normalized homogeneous polynomials in x and y irreducible $\mathrm{Mod}\,p$ of degree 1, 2 and 3 equals $p+1$, $\frac{1}{2}p(p-1)$ and $\frac{1}{3}p(p-1)(p+1)$ respectively. The lemma now follows by an elementary counting process.

Definition (only used in this section). *$S_1 = S_{1,p}$ denotes the set of forms $F \in \Phi$ satisfying*

$$a \not\equiv 0\,(\mathrm{mod}\,p), \quad b \equiv c \equiv 0\,(\mathrm{mod}\,p), \quad d \equiv 0\,(\mathrm{mod}\,p^2).$$

$S_2 = S_{2,p}$ denotes the set of forms $F \in \Phi$ satisfying

$$b \not\equiv 0\,(\mathrm{mod}\,p), \quad a \equiv c \equiv 0\,(\mathrm{mod}\,p), \quad d \equiv 0\,(\mathrm{mod}\,p^2).$$

Σ_1 and Σ_2 denote the set of forms in Φ which are equivalent to at least one F in S_1 and S_2 respectively.

Note that $F \in \Sigma_1 \Rightarrow (F,p) = (1^3)$ and $F \in \Sigma_2 \Rightarrow (F,p) = (1^2 1)$.

Lemma 2.
$$A(\Sigma_1; p^2) = p^{-1}(p^2+1)^{-2},$$
$$A(\Sigma_2; p^2) = (p^2+1)^{-2}.$$

Proof. It is clear that

$$A(S_1; p^2) = A(S_2; p^2) = p^{-1}(p+1)^{-1}(p^2+1)^{-1}.$$

Let $\begin{pmatrix} k & l \\ m & n \end{pmatrix}$ be a linear substitution $\mathrm{mod}\,p^2$ of determinant ± 1. Then if $F \in S_1$,

$$F(kx+ly, mx+ny) \equiv a(kx+ly)^3 \quad (\mathrm{Mod}\,p);$$

so this form lies in S_1 only if $l \equiv 0\,(\mathrm{mod}\,p)$. Conversely, if $l \equiv 0\,(\mathrm{mod}\,p)$,

$$F(kx+ly, mx+ny) \equiv a(kx+ly)^3 + ckx(mx+ny)^2 + b(kx)^2(mx+ny) \quad (\mathrm{Mod}\,p^2)$$

and the form lies in S_1. The unimodular substitutions $\mathrm{mod}\,p^2$ with $l \equiv 0\,(\mathrm{mod}\,p)$ form a subgroup of index $p+1$ of the group of all unimodular substitutions $\mathrm{mod}\,p^2$. Hence

$$A(\Sigma_1; p^2) = (p+1)\,A(S_1; p^2) = p^{-1}(p^2+1)^{-1}.$$

Similarly, if $F \in S_2$,

$$\begin{aligned} F(kx+ly, mx+ny) &\equiv b(kx+ly)^2(mx+ny) \\ &\equiv bk^2mx^3 + bk(2lm+kn)x^2y + bl(lm+2kn)xy^2 + bl^2ny^3 \\ &\equiv a'x^3 + b'x^2y + c'xy^2 + d'y^3 \quad (\mathrm{Mod}\,p) \quad \text{say.} \end{aligned}$$

Assume this form lies in S_2. Then $p \nmid b'$, hence $p \nmid k$. As $p|a'$, $p \nmid b$, we have $p|m$. As $p \nmid b'$, $p|m$, we have $p \nmid n$. As $p|d'$, $p \nmid bn$, we have $p|l$.

Conversely, if $l \equiv m \equiv 0 \pmod p$,

$$\begin{aligned} F(kx+ly, mx+ny) &\equiv ak^3x^3 + b(kx+ly)^2(mx+ny) + ckn^2xy^2 + dn^3y^3 \\ &\equiv (ak^3 + bk^2m)x^3 + b(k^2n + 2klm)x^2y \\ &\quad + (b(2kln + l^2m) + ckn^2)xy^2 + (bl^2n + dn^3)y^3 \pmod{p^2}. \end{aligned}$$

Thus this form belongs to S_2. The unimodular matrices with $l \equiv m \equiv 0 \pmod p$ form a subgroup of index $p(p+1)$ in the group of all unimodular matrices $\bmod p^2$. Hence

$$A(\Sigma_2; p^2) = p(p+1)A(S_2; p^2) = (p^2+1)^{-2}.$$

LEMMA 3. *$\Phi = V_p \cup T_p(1^3) \cup \Sigma_2$ for all p, and no two sets on the right have an element in common.*

Proof. It is clear that each F with $(F, p) \neq (1^2 1)$ belongs to one and only one of these sets. Hence we need only prove the lemma for $F \in T(1^2 1)$. Such F may be assumed to have coefficients a, b, c, d such that

$$a \equiv c \equiv d \equiv 0 \pmod p, \quad b \not\equiv 0 \pmod p.$$

Then

$$D \equiv -4b^3d \pmod{p^2}.$$

Thus for $p \neq 2$, $D \equiv 0 \pmod{p^2}$ if and only if $d \equiv 0 \pmod{p^2}$. This shows that every form of $T_p(1^2 1)$ lies either in V_p or in Σ_2.

For $p = 2$ we have

$$D \equiv b^2c^2 - 4b^3d \equiv 4((\tfrac{1}{2}c)^2 - bd) \pmod{16}.$$

Thus $d \equiv 0 \pmod 4$ if and only if $D \equiv 0$ or $4 \pmod{16}$. This proves the lemma.

LEMMA 4. $A(V_p; p^2) = (p^2-1)(p^2+1)^{-1}$ *for all* p.

Proof. By lemma 3

$$1 = A(V_p; p^2) + A(T_p(1^3); p^2) + A(\Sigma_2; p^2).$$

By lemmas 1 and 2

$$A(T_p(1^3); p^2) = (p^2+1)^{-1}, \quad A(\Sigma_2; p^2) = (p^2+1)^{-1},$$

and the result follows.

LEMMA 5. $A(U_p; p^2) = (p^3-1)p^{-1}(p^2+1)^{-1}$ *for all* p.

Proof. It follows from the definition of U_p that

$$T_p(1^3) = (T_p(1^3) \cap U_p) \cup \Sigma_1, \quad U_p = V_p \cup (T_p(1^3) \cap U_p).$$

As $\Sigma_1 \cap U_p$ is empty, we have

$$U_p \cup \Sigma_1 = V_p \cup T_p(1^3),$$

$$\begin{aligned} A(U_p; p^2) &= A(V_p; p^2) + A(T_p(1^3); p) - A(\Sigma_1; p^2) \\ &= (p^2-1)(p^2+1)^{-1} + (p^2+1)^{-2} - p^{-1}(p^2+1)^{-1} \end{aligned}$$

by lemmas 4, 1 and 2. Hence the assertion follows.

Lemma 6. *If* $(F,p) = (1^3)$, $p \neq 3$ *then* $F \in U_p$ *if and only if* $D \not\equiv 0 \pmod{p^3}$. *If* $(F, 3) = (1^3)$, $F \in U_3$, *then* $D \not\equiv 0 \pmod{729}$.

Proof. Assume $a \not\equiv 0 \pmod{p}$, $b \equiv c \equiv d \equiv 0 \pmod{p}$. Then for $p \neq 3$

$$D \equiv -27a^2d^2 \pmod{p^3}.$$

Hence $D \equiv 0 \pmod{p^3}$ if and only if $d \equiv 0 \pmod{p^2}$.

For $p = 3$, put $b = 3\beta$, $c = 3\gamma$, $d = 3\delta$, so that $3 \nmid \delta$. Then

$$D = 81\beta^2\gamma^2 + 486a\beta\gamma\delta - 243a^2\delta^2 - 324\beta^3\delta - 108\gamma^3 a.$$

If $3 \nmid \gamma$, $$D \equiv -108\gamma^3 a \pmod{81}.$$

If $3 | \gamma$, $$D \equiv -81\delta(3a^2\delta - 4\beta^3) \pmod{729}.$$

Hence in either case $D \not\equiv 0 \pmod{729}$.

4. An auxiliary proposition

In order to apply a simple sieve method later, we require

Proposition 1. $N(-X, X; W_p) = O(xp^{-2})$ *as* $X \to \infty$.

We first prove

Lemma 7. $$\sum_{|\Delta_2|<X} h_3^*(\Delta_2) = O(X) \text{ as } X \to \infty,$$

where Δ_2 *runs through the discriminants of quadratic fields.*

Proof. This lemma follows from our old theorem

$$N_3(-X, X) = O(X) \quad \text{as} \quad X \to \infty$$

(Davenport & Heilbronn 1969) as theorem 3 will follow from theorem 1. (See §7.)

We now introduce the Hessian $H(x,y)$ of a given cubic form $F(x,y)$. H is defined by the relation

$$H(x,y) = -\tfrac{1}{4}(F_{xx}F_{yy} - F_{xy}^2),$$

where the lower indices denote partial derivatives. It is well known that $H(x,y)$ is a covariant of $F(x,y)$ with respect to linear substitutions of determinant 1. A simple calculation gives

$$H(x,y) = (bx+cy)^2 - (3ax+by)(cx+3dy)$$
$$= Px^2 + Qxy + Ry^2, \quad \text{say,}$$

where $P = b^2 - 3ac$, $Q = bc - 9ad$, $R = c^2 - 3bd$. An easy calculation shows the discriminant Δ of H is given by

$$\Delta = Q^2 - 4PR = -3D.$$

The class of H is uniquely determined by the class of F, but the converse is not necessarily true. The formula for Δ shows H is reducible if and only if $-3D$ is a square. H is primitive if and only if for all primes p $(F,p) \neq (1^3)$. So we put

$$M = (P, Q, R), \quad P = MP_1, \quad Q = MQ_1, \quad R = MR_1,$$

$$H_1(x,y) = P_1x^2 + Q_1xy + R_1y^2,$$

and this quadratic form has discriminant

$$\Delta_1 = Q_1^2 - 4P_1R_1 = M^{-2}\Delta = -3M^{-2}D.$$

The explicit definition of $H(x,y)$ leads immediately to the identities

$$H_1(b, -3a) = MP_1^2,$$
$$H_1(c, -b) = MP_1R_1,$$
$$H_1(3d, -c) = MR_1^2.$$

LEMMA 8. *Let $k > 0$, $M > 0$, $M \in \mathbf{Z}$. Let $B = B(k,M)$ denote the number of classes of forms in Φ with Hessian $H(x,y) = M(kx+ly)y$, where $0 \leqslant l < k$, $(l,k) = 1$. Then*

$$B \leqslant 2k\tau(M).$$

Moreover, if p is a prime such that $p|k$, $p^2 \nmid M$, then

$$B \leqslant 6kp^{-1}\tau(M).$$

Proof. Let F be a form in Φ with Hessian

$$H(x,y) = M(kx+ly)\,y = MH_1(x,y), \quad \text{say.}$$

We may assume that $a > 0$. The equations

$$H_1(b, -3a) = (kb-3al)\,(-3a) = MP_1^2 = 0,$$
$$H_1(c, -b) = (kc-bl)\,(-b) = MP_1R_1 = 0$$

yield $b = 3k^{-1}la$ and, if $l \neq 0$, $c = 3k^{-2}l^2a$. If $l = 0$, the third equation

$$H_1(3d, -c) = (3kd-cl)\,(-c) = MR_1^2 = Ml^2$$

yields $c = 0$ because $d \neq 0$. Hence F has the form

$$F(x,y) = a(x+k^{-1}ly)^3 \pm (9a)^{-1}Mky^3,$$

the last coefficient being determined by the value of

$$D = -\tfrac{1}{3}M^2k^2 = -27a^2((9a)^{-1}Mk)^2.$$

As the coefficients of F are integers, we obtain the congruences

$$3al^2 \equiv 0 \pmod{k^2}, \quad 9a^2l^3 \pm Mk^4 \equiv 0 \pmod{9ak^3}.$$

If $k = 1$, the second congruence shows that $a|M$, so that we have $\tau(M)$ choices for a and one choice for l which proves our result.

If $k > 1$, the first congruence shows that $k^2|3a$, so we can put $3a = sk^2$. The second congruence now reads

$$s^2l^3 \pm M \equiv 0 \pmod{3sk}.$$

This implies that $s|M$ and we can find at most $\tau(M)$ values of a and at most k values of l. This proves our first result for $k > 1$.

Now assume the existence of p with $p|k$, $p^2\nmid M$. Then $p\nmid s$ and the congruence

$$s^2l^3 \pm M \equiv 0 \pmod p$$

has at most six solutions mod p. Hence the original congruence has at most $6kp^{-1}$ solutions in $0 < l < k$. This proves the last assertion of the lemma.

Lemma 9. *If $M > 0$ and $H_1(x,y)$ are given, and if Δ_1 is not a square, then there are at most $18\tau(M)$ classes of irreducible primitive cubic forms with Hessian equivalent to $MH_1(x,y)$.*

Proof. As $H_1(x,y)$ is primitive we may assume that P_1 is a prime. Assume first that $\Delta_1 < 0$. Then

$$H_1(b,-3a) = MP_1^2.$$

Hence by the theory of definite primitive quadratic forms, the number of representations of MP_1^2 is at most $6\tau(MP_1^2) \leqslant 18\tau(M)$.

Thus there are at most $18\tau(M)$ choices for a, b. As a, b, P_1, Q_1 determine c and d uniquely (since $a \neq 0$), the lemma follows for $\Delta < 0$.

For a positive Δ the situation is not so simple, as the form $H_1(x,y)$ has a cyclic infinite group of automorphs.

We write $H(x,y)$ in the form

$$H(x,y) = MH_1(x,y) = MP_1(x+\theta y)(x+\theta' y)$$

where

$$\theta = (2P_1)^{-1}(Q_1+\sqrt{\Delta_1}),\ \theta' = (2P_1)^{-1}(Q_1-\sqrt{\Delta_1}).$$

If $H(x,y)$ is the Hessian of $F(x,y)$, we have

$$3(\theta-\theta')F(x,y) = (b-3a\theta')(x+\theta y)^3-(b-3a\theta)(x+\theta' y)^3.$$

Let $\epsilon > 1$ be the smallest unit in $\boldsymbol{Q}(\sqrt{\Delta_1})$ which can be written in the form

$$\epsilon = \tfrac{1}{2}(e_1+e_2\sqrt{\Delta_1}).$$

The non-trivial automorphs of $H(x,y)$ are then generated by the substitution S

$$x^*+\theta y^* = \epsilon(x+\theta y),$$
$$x^*+\theta' y^* = \epsilon^{-1}(x+\theta' y).$$

Hence

$$b^*-3a^*\theta = \epsilon^3(b-3a\theta),$$
$$b^*-3a^*\theta' = \epsilon^{-3}(b-3a\theta').$$

This shows that if the x, y space is transformed by S, the b, $-3a$ space is transformed by S^3. Thus we need only count solutions of

$$H_1(b,-3a) = MP_1^2$$

subject to equivalence by S^{3n}, as two solutions which differ only by S^{3n} lead to equivalent forms F. The number of solutions not equivalent by S^n are at most $2\tau(MP_1^2)$, hence the number of solutions not equivalent by S^{3n} is at most $6\tau(MP_1^2) \leqslant 18\tau(M)$, as P_1 may be assumed to be a prime.

Lemma 10. *Let $M > 0$ and $\Delta_1 \equiv 0$ or $1 \pmod 4$ be elements of $\mathbf{Z}$, Δ_1 not a square. Then there exist at most $3\tau(M)\,h_3^*(\Delta_1)$ classes of primitive quadratic forms*

$$H_1(x,y) = P_1x^2+Q_1xy+R_1y^2 \quad \textit{with} \quad Q_1^2-4P_1R_1 = \Delta_1,$$

such that MH_1 is the Hessian of a form $F \in \Phi$.

Proof. Let $F(x,y)$ be a form in Φ with Hessian $MH_1(x,y)$. Then we have

$$P_1b^2 - 3Q_1ba + 9R_1a^2 = MP_1^2.$$

Without loss of generality we may assume that P_1 is a prime.

We now consider classes of equivalent primitive quadratic forms of discriminant Δ_1. Let η be the class of H_1 and let $\mu_1, \ldots, \mu_t$ be the classes which represent M. It follows from the theory of composition of quadratic forms that $1 \leqslant t \leqslant \tau(M)$. Hence there exists at least one s in $1 \leqslant s \leqslant t$ such that at least one of the following three relations holds:

$$\eta = \mu_s \quad \text{or} \quad \eta = \mu_s \eta^2 \quad \text{or} \quad \eta = \mu_s \eta^{-2}.$$

The number of such η is at most

$$t(2 + h_3^*(\Delta_1)) \leqslant \tau(M)\,(2 + h_3^*(\Delta_1)) \leqslant 3\tau(M)\,h_3^*(\Delta_1).$$

Proof of proposition 1. We first deal with those classes for which $-3D$ is a square. We have to find an upper bound for the sum

$$\sum_{\substack{Mk<(3X)^{\frac{1}{2}} \\ p|Mk}} B(k,M) = \sum_{Mk<(3X)^{\frac{1}{2}}p^{-1}} B(k,pM) + \sum_{\substack{Mk<(3X)^{\frac{1}{2}}p^{-1} \\ p\nmid M}} B(pk,M).$$

To the first sum we apply the first estimate in lemma 8, to the second sum the second estimate. Then our bound is

$$\begin{aligned}
&\leqslant \sum_{kM<(3X)^{\frac{1}{2}}p^{-1}} (2k\tau(pM) + 6k\tau(M)) \\
&\leqslant 10 \sum_{M<(3X)^{\frac{1}{2}}p^{-1}} \tau(M) \sum_{k<(3X)^{\frac{1}{2}}p^{-1}M^{-1}} k \\
&\leqslant 10(3X)\,p^{-2} \sum_{M=1}^{\infty} \tau(M)\,M^{-2} \\
&= O(Xp^{-2}).
\end{aligned}$$

Now we have to count those classes for which $-3D$ is not a square and the Hessian is irreducible. That means, by virtue of lemma 9 and lemma 10 we have to find an upper bound for the sum

$$\sum_{\substack{|M^2\Delta_1|\leqslant 3X \\ p^2|M^2\Delta_1}} 54\tau^2(M)\,h_3^*(\Delta_1),$$

where Δ_1 is restricted to discriminants of quadratic forms. Each such Δ_1 can be factorized uniquely in the form $\Delta_1 = L^2\Delta_2$, where $L > 0$, $L \in \mathbf{Z}$ and Δ_2 is discriminant of a quadratic field. For $p = 2$ the proposition follows from Davenport's theorem, so we may assume $p \neq 2$. Hence $p^2 \nmid \Delta_2$, and $p^2|M^2\Delta_1$ implies $p|ML$.

To express $h_3^*(\Delta_1)$ by $h_3^*(\Delta_2)$ exactly is difficult; it is however well known that

$$h_3^*(\Delta_1)\,|\,3^n h_3^*(\Delta_2),$$

where n denotes the number of distinct prime divisors of L. Hence

$$h_3^*(\Delta_1) \leqslant \tau^2(L)\,h_3^*(\Delta_2).$$

Substituting this in our formula for the upper bound we obtain

$$54 \sum_{\substack{|M^2L^2\Delta_2|<3X \\ p|ML}} \tau^2(M)\,\tau^2(L)\,h_3^*(\Delta_2).$$

By virtue of lemma 7 this is majorized by

$$O(X) \sum_{\substack{M=1 \\ p|ML}}^{\infty} \sum_{L=1}^{\infty} \tau^2(M)\,\tau^2(L)\,M^{-2}L^{-2} = O(Xp^{-2}).$$

5. Global densities

The starting-point of this section is the

THEOREM (Davenport 1951*a*, *b*)

$$N(0,X;\Phi) = \tfrac{5}{4}\pi^{-2}X + O(X^{\frac{15}{16}}),$$
$$N(-X,0;\Phi) = \tfrac{15}{4}\pi^{-2}X + O(X^{\frac{15}{16}}).$$

Actually we require a refinement of this theorem. Let $m \geqslant 1$ and S_m be a set of forms in ϕ which are defined by conditions on the residue classes of $a, b, c, d \pmod m$. Moreover let S_m be a union of equivalence classes of Φ. Then

$$\lim_{X\to\infty} X^{-1}N(0,X;S_m) = \tfrac{5}{4}\pi^{-2}A(S_m;m),$$
$$\lim_{X\to\infty} X^{-1}N(-X,0;S_m) = \tfrac{15}{4}\pi^{-2}A(S_m;m).$$

This extension is proved in exactly the same way as the original theorem. It does not hold uniformly in m.

Let Y be a large integer in $\mathbf{Z}$, and let

$$P_Y = \prod_{p<Y} p.$$

Then as $X\to\infty$, for fixed Y,

$$\begin{aligned} X^{-1}N(X,0;\bigcap_{p<Y} U_p) &\to \tfrac{5}{4}\pi^{-2}A(\bigcap_{p<Y} U_p;P_Y^2) \\ &= \tfrac{5}{4}\pi^{-2}\prod_{p<Y} A(U_p;p^2) \\ &= \tfrac{5}{4}\pi^{-2}\prod_{p<Y}(p^3-1)\,p^{-1}(p^2+1)^{-1} \end{aligned}$$

by lemma 5. Thus

$$\limsup_{X\to\infty} X^{-1}N(X,0;U) \leqslant \tfrac{5}{4}\pi^{-2}\prod_{p<Y}(p^3-1)\,p^{-1}(p^2+1)^{-1}.$$

As this is true for all $Y > 0$, we may replace the product by the infinite product over all primes. This gives

$$\begin{aligned} \limsup_{X\to\infty} X^{-1}N(X,0;U) &\leqslant \tfrac{5}{4}\pi^{-2}\prod_{p}(1-p^{-3})(1+p^{-2})^{-1} \\ &= \tfrac{5}{4}\pi^{-2}\zeta(3)^{-1}\zeta(2)^{-1}\zeta(4) = \tfrac{5}{4}\pi^{-2}\zeta(3)^{-1}(6\pi^{-2})(\pi^4/90) \\ &= (12\zeta(3))^{-1}. \end{aligned}$$

To obtain a lower bound for $N(0,X;U)$ we observe that

$$\bigcap_{p<Y} U_p \subset (U \cup \bigcup_{p\geq Y} W_p).$$

Hence, using proposition 1,

$$\tfrac{5}{4}\pi^{-2} \prod_{p<Y} (p^3-1)\,p^{-1}(p^2+1)^{-1} \leqslant \liminf_{X\to\infty} (X^{-1}N(0,X;U)+X^{-1} \sum_{p\geqslant Y} N(0,X;W_p))$$

$$\leqslant \liminf_{X\to\infty} (X^{-1}N(0,X;U)) + O\sum_{p\geqslant Y} p^{-2}.$$

Letting Y tend to infinity, this gives

$$\liminf_{X\to\infty} X^{-1}N(0,X;U) \geqslant \tfrac{5}{4}\pi^{-2} \prod_{p} (p^3-1)\,p^{-1}(p^2+1)^{-1} = (12\zeta(3))^{-1}.$$

The same argument works for negative discriminants. We have thus proved

PROPOSITION 2. $$\lim_{X\to\infty} X^{-1}N(0,X;U) = (12\zeta(3))^{-1},$$

$$\lim_{X\to\infty} X^{-1}N(-X,0;U) = (4\zeta(3))^{-1}.$$

Applying the same argument to V instead of U, we note that the relation

$$\bigcap_{p<Y} V_p \subset (V \cup \bigcup_{p\geqslant Y} W_p)$$

still holds. Also by lemma 4

$$A(V_p;p^2) = (p^2-1)(p^2+1)^{-1},$$

$$\tfrac{5}{4}\pi^{-2} \prod_{p} (1-p^{-2})(1+p^{-2})^{-1} = \tfrac{5}{4}\pi^{-2}\zeta(4)\,\zeta(2)^{-2}$$

$$= \tfrac{5}{4}\pi^{-2}(\pi^4/90)(36/\pi^4) = \tfrac{1}{2}\pi^{-2}.$$

This gives

PROPOSITION 3. $$\lim_{X\to\infty} X^{-1}N(0,X;V) = (2\pi^2)^{-1},$$

$$\lim_{X\to\infty} X^{-1}N(-X,0;V) = 3(2\pi^2)^{-1}.$$

6. THE FUNDAMENTAL MAPPING

Let K be a cubic field over Q. In our previous paper we attached to each K a binary cubic form in the following way. Let 1, ω, ν be an integral basis of K. Put

$$F_K(x,y) = \mathfrak{d}_K^{-\frac{1}{2}}\,\mathfrak{d}^{\frac{1}{2}}(\omega x+\nu y),$$

where $\mathfrak{d}_K$ denotes the absolute discriminant of K. We proved

(1) $F_K \in \Phi$.
(2) F_K is uniquely determined by K apart from equivalence.
(3) If K' is conjugate to K, $F_{K'}$ is equivalent to F_K.
(4) $D(F_K) = \mathfrak{d}_K$.
(5) If K_1 is not conjugate to K, then F_{K_1} is not even rationally equivalent to F_K.

LEMMA 11. *The rational prime p factorizes in K according to the following table:*

$$(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \quad \textit{if} \quad (F_K, p) = (111),$$
$$(p) = \mathfrak{p}_1\mathfrak{p}_2 \quad \textit{if} \quad (F_K, p) = (12),$$
$$(p) = (p) \quad \textit{if} \quad (F_K, p) = (3),$$
$$(p) = \mathfrak{p}^3 \quad \textit{if} \quad (F_K, p) = (1^3),$$
$$(p) = \mathfrak{p}_1^2\mathfrak{p}_2 \quad \textit{if} \quad (F_K, p) = (1^2\,1).$$

Proof. Assume first that a, the coefficient of x^3 in F_K, is not divisible by p. Consider the polynomial

$$f(x) = x^3 + bx^2 + acx + a^2 d.$$

This polynomial is irreducible over Q, and has a zero in K. Its discriminant equals $a^2\mathfrak{d}_K$. Hence, by the Kummer–Dedekind theorem, $f(x)$ factorizes Mod p in the same way as p factorizes in K. As $f(x)$ factorizes Mod p in the same way as $F_K(x, y)$, our lemma is proved.

It remains to deal with the case that $p|a$ for all forms equivalent to F_K. This happens only if $p^2\mathfrak{d}_K|\mathfrak{d}(\alpha)$ for all integers α in K, i.e. if p is a 'non-essential divisor' of the discriminant of K. It is well known that this case arises only if $p = 2$, $\mathfrak{d}_K \equiv 1 \pmod 2$ and 2 factorizes completely in K. Then $a \equiv d \equiv 0 \pmod 2$, $D \equiv 1 \pmod 2$, hence $b \equiv c \equiv 1 \pmod 2$; $F_K(x, y) \equiv xy(x+y)$ (Mod 2), i.e. $(F, 2) \equiv (111)$. This observation completes the proof of the lemma.

LEMMA 12. $F_K \in U$.

Proof. We state a few well-known facts on cubic fields (Hasse 1930). If K is cyclic, the discriminant $\mathfrak{d}_K$ of K has the form $\mathfrak{d}_K = f^2$; if K is not cyclic, $\mathfrak{d}_K$ has the form $\mathfrak{d}_K = \Delta_2 f^2$, where Δ_2 is the discriminant of a quadratic field. In both cases $p^2 \nmid f$ if $p \neq 3$; and $(\Delta_2, f) = 1$ or 3. Further $p^2 \nmid \Delta_2$ if $p \neq 2$. A prime p ramifies completely in K if and only if $p|f$.

We want to show that $F_K \in U_p$ for all p. If $p^2 \nmid \mathfrak{d}_K$, this follows at once from the definition of U_p. Hence we may assume that $\mathfrak{d}_K \equiv 0 \pmod{p^2}$.

If $p > 3$, the last congruence implies $p|f$, and p ramifies completely in K, so that by lemma 11 $(F_K, p) = (1^3)$. As $p^3 \nmid \mathfrak{d}_K$, it follows from lemma 6 that $F_K \in U_p$.

If $p = 2$, we have either $4|\Delta_2$ or $2|f$. If $4|\Delta_2$, then $\Delta_2 \equiv 8$ or $12 \pmod{16}$, $f^2 \equiv 1 \pmod 8$, hence $\mathfrak{d}_K \equiv 8$ or $12 \pmod{16}$, $F_K \in V_2 \subset U_2$. If $2|f$, 2 ramifies completely in K, hence by lemma 11 $(F_K, 2) = (1^3)$. As $\mathfrak{d}_K \equiv 4 \pmod 8$, it follows from lemma 6 that $F_K \in U_2$.

There remains only the case $p = 3$, $f \equiv 0 \pmod 3$. Let $\mathfrak{p}$ denote the unique prime ideal in K which divides 3. Because 3 is not a 'non-essential divisor' of the discriminant, there exists in K an integer α such that

$$3\mathfrak{d}_K \nmid \mathfrak{d}(\alpha).$$

Without loss of generality we may assume that $\alpha \equiv 0 \pmod{\mathfrak{p}}$, otherwise consider $\alpha - 1$ or $\alpha + 1$. Hence $\operatorname{tr}(\alpha) \equiv 0 \pmod 3$. It is easy to verify the identity

$$\mathfrak{d}(\alpha^2) = \mathfrak{d}(\alpha)\,\mathrm{Nm}^2(\operatorname{tr}(\alpha) - \alpha).$$

If $\alpha \not\equiv 0 \pmod{\mathfrak{p}^2}$, then

$$\mathrm{Nm}(\mathrm{tr}(\alpha)-\alpha) \equiv \pm 3 \pmod 9,$$

$$\mathfrak{d}(\alpha^2)\,\mathfrak{d}_K^{-1} = \mathfrak{d}(\alpha)\,\mathfrak{d}_K^{-1}\,\mathrm{Nm}^2(\mathrm{tr}(\alpha)-\alpha) \equiv \pm 9 \pmod{27}.$$

This means that $F_K(x,y)$ represents a number $\equiv \pm 3 \pmod 9$, i.e. $F_K(x,y) \in U_3$.

If $\alpha \equiv 0 \pmod{\mathfrak{p}^2}$, our identity gives

$$\mathfrak{d}(\tfrac{1}{3}\alpha^2) = 3^{-6}\,\mathfrak{d}(\alpha^2) = 3^{-6}\,\mathfrak{d}(\alpha)\,\mathrm{Nm}^2(\mathrm{tr}(\alpha)-\alpha),$$

$$\mathfrak{d}(\tfrac{1}{3}\alpha^2)\,\mathfrak{d}_K^{-1} = \mathfrak{d}(\alpha)\,\mathfrak{d}_K^{-1}\{3^{-3}\mathrm{Nm}(\mathrm{tr}(\alpha)-\alpha)\}^2$$

and, since $\frac{1}{3}\alpha^2$ is an integer in K,

$$3^3 | \mathrm{Nm}(\mathrm{tr}(\alpha)-\alpha).$$

This implies that $3|\alpha$, and therefore

$$\mathfrak{d}(\tfrac{1}{3}\alpha) = 3^{-6}\,\mathfrak{d}(\alpha) \equiv 0 \pmod{\mathfrak{d}_K},$$

$$\mathfrak{d}(\alpha) \equiv 0 \pmod{3^6\,\mathfrak{d}_K}$$

which is a contradiction.

LEMMA 13. *Let F_1 and F_2 be two forms in U which are rationally equivalent. Then they are equivalent.*

Proof. Rational equivalence between F_1 and F_2 means explicitly that

$$F_1(x_1, y_1) = \sigma F_2(x_2, y_2),$$

$$(x_1, y_1) = M(x_2, y_2),$$

where $\sigma \neq 0$ is rational and M is a non-singular 2 by 2 matrix over $\mathbf{Z}$. If we replace F_1 by an equivalent form, M will be multiplied by a unimodular matrix on the left. Similarly, replacing F_2 by an equivalent form means multiplication of M with a unimodular matrix on the right.

Thus we may replace M by $M_1 M M_2$, where M_1 and M_2 are unimodular. Elementary divisor theory tells us that we can choose M_1 and M_2 in such a way that

$$M_1 M M_2 = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix},$$

where $m = |\det(M)|$. If $m = 1$, our forms are equivalent.

Otherwise, there exists a prime $p|m$. Write $m = p^l m_0$, $\sigma = p^k \sigma_0$ so that $l \geqslant 1$, and m_0, σ_0 are prime to p. Then our transformation takes the form

$$F_1(p^l m_0 x, y) = p^k \sigma_0 F_2(x, y).$$

Equating coefficients we obtain

$$a_1 = p^{k-3l}\tau_a a_2,$$
$$b_1 = p^{k-2l}\tau_b b_2,$$
$$c_1 = p^{k-l}\tau_c c_2,$$
$$d_1 = p^k \tau_d d_2,$$

where $\tau_a, \tau_b, \ldots$ are rationals prime to p.

If $k-l>0$, we have $p|c_1$, $p^2|d_1$. If $k-l \leqslant 0$, we have $p|b_2$, $p^2|a_2$. Because of symmetry, we may restrict ourselves to the first case, $p|c_1$, $p^2|d_1$ implies $p^2|D_1$. As $F_1 \in U_p$, it follows that $(F_1, p) = (1^3)$, and therefore $p|b_1$. As $F_1 \in U_p$ and $p^2|D_1$, the congruence

$$F_1(x,y) \equiv ep \pmod{p^2}$$

has a solution for some $e \not\equiv 0 \pmod{p}$. As $b_1 \equiv c_1 \equiv d_1 \equiv 0 \pmod{p}$, it follows that $x \equiv 0 \pmod{p}$. But this implies

$$F_1(x,y) \equiv c_1 xy^2 + d_1 y^3 \equiv 0 \pmod{p^2},$$
$$e \equiv 0 \pmod{p}.$$

This contradiction completes the proof of the lemma.

Lemma 14. *To every $F \in \Phi$ there belongs a cubic field K such that F and F_K are rationally equivalent.*

Proof. Write F in the form

$$F(x,y) = a(x-\lambda y)(x-\lambda' y)(x-\lambda'' y).$$

Then λ generates a cubic field K. We can write F_K in the form

$$F_K(x,y) = a_K(x-\mu y)(x-\mu' y)(x-\mu'' y),$$

where $\mu \in K$. If K is not cyclic, μ is unique, but if K is cyclic any of the three conjugates can be used. As λ and μ are irrationals in K, there exists a relation $k\lambda + l - m\mu\lambda - n\mu = 0$, $(k,l,m,n) = 1$, which is unique apart from a factor ± 1. Thus we have

$$\mu = (k\lambda + l)(m\lambda + n)^{-1}$$

and this also holds if we replace λ, μ by their two pairs of conjugates.

The transformation

$$x^* = kx + ly, \quad y^* = mx + ny$$

transforms the form $F(x,y) = a(x-\lambda y)(x-\lambda' y)(x-\lambda'' y)$

into a form $\rho(x^* - \mu y^*)(x^* - \mu' y^*)(x^* - \mu'' y^*)$,

which is a constant multiple of $F_K(x^*, y^*)$.

Proposition 4. *There exists a 1–1 mapping Λ of triplets of conjugate cubic fields K onto the equivalence classes of U. And Λ preserves the discriminant.*

Proof. The map Λ: $K \to F_K$ maps the triplets into classes of U by lemma 12. By lemmas 14 and 13 every class in U contains an F_K. And it was stated at the beginning of this section that distinct triplets are mapped into distinct classes of U, and that $D(F_K) = \mathfrak{d}_K$.

7. Proof of theorems 1, 2 and 3

Proof of theorem 1. It follows from proposition 4 that

$$N_3(\xi,\eta) = N(\xi,\eta; U).$$

This identity in conjunction with proposition 2 gives theorem 1.

Proof of theorem 2. Let p be a fixed prime. By virtue of lemma 11 the mapping considered in the preceding proof maps the classes of forms in $U \cap T_p(111)$; $U \cap T_p(3)$ and $U \cap T_p(12)$ into cubic fields in which p factorizes as $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $(p) = (p)$, $(p) = \mathfrak{p}_1\mathfrak{p}_2$ respectively.

It is easily seen that the relative density of our 3 classes in U equals

$$A(T_p(111); p^2)A^{-1}(U_p; p^2), \quad \text{etc.}$$

By lemmas 1 and 5 these three relative densities are

$$\tfrac{1}{6}(1+p^{-1}+p^{-2})^{-1}, \quad \tfrac{1}{3}(1+p^{-1}+p^{-2})^{-1}, \quad \tfrac{1}{2}(1+p^{-1}+p^{-2})^{-1}$$

respectively.

As the cyclic cubic fields have relative density 0, they may be ignored. For non-cyclic cubic fields it is well known that the three types of factorization correspond to the three values I, A_3–I, S_3–A_3 of the Frobenius–Artin symbol $\{(K_6/Q)/p\}$.

Proof of theorem 3. Let K be a cubic field in which no prime ramifies completely, so that K is automatically not cyclic. This means, in the notation used in the proof of lemma 12, that $f = 1$ and that $\mathfrak{d}_K = \Delta_2$, where Δ_2 is discriminant of a quadratic field. For a given Δ_2 the number of triplets of such cubic fields K equals (Hasse 1930)

$$\tfrac{1}{2}(h_3^*(\Delta_2)-1).$$

On the other hand, the mapping Λ maps these triplets into the classes of V. Hence

$$\tfrac{1}{2}\sum_{\xi<\Delta_2<\eta}(h_3^*(\Delta_2)-1) = N(\xi,\eta;V).$$

An easy calculation shows that, as $X\to\infty$,

$$X^{-1}\sum_{0<\Delta_2<X}1\to 3\pi^{-2},$$

$$X^{-1}\sum_{-X<\Delta_2<0}1\to 3\pi^{-2}.$$

Hence by proposition 3

$$\lim_{X\to\infty}X^{-1}\sum_{0<\Delta_2<X}(h_3^*(\Delta_2)-1) = \lim_{X\to\infty}2X^{-1}N(0,X;V)$$

$$= \pi^{-2} = \lim_{X\to\infty}X^{-1}\sum_{0<\Delta_2<X}\tfrac{1}{3};$$

$$\lim_{X\to\infty}X^{-1}\sum_{-X<\Delta_2<0}(h_3^*(\Delta_2)-1) = \lim_{X\to\infty}2X^{-1}N(-X,0;V)$$

$$= 3\pi^{-2} = \lim_{X\to\infty}X^{-1}\sum_{-X<\Delta_2<0}1.$$

This completes the proof of our theorems.

References

Davenport, H. 1951 *a* On the class-number of binary cubic forms (I). *J. Lond. Math. Soc.* **26**, 183–192. (Corrigendum, *ibidem* **27**, 512.)

Davenport, H. 1951 *b* On the class-number of binary cubic forms (II). *J. Lond. Math. Soc.* **26**, 192–198.

Davenport, H. & Heilbronn, H. 1969 On the density of discriminants of cubic fields. *Bull. Lond. Math. Soc.* **1** (1969), 345–348.

Hasse, H. 1930 Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. *Math. Z.* **31**, 565–582.