NOTES ON DAVENPORT-HEILBRONN'S RESULTS ON CUBIC FIELDS

FRANK THORNE

Abstract. These notes describe, in an extremely sketchy manner, the result of Davenport-Heilbronn [2] proving an asymptotic for the number of cubic fields of prescribed discriminant.

1. Introduction

Definition 1.1. *We let $N_3(\xi, \eta)$ denote the number of cubic fields K with discriminant Δ_K satisfying $\xi < \Delta_K < \eta$, where a triplet of conjugate fields is counted once only.*

If Ψ is an $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of irreducible binary cubic forms, we let $N(\xi, \eta; \Psi)$ denote the number of equivalence classes of forms in Ψ with discriminant Δ satisfying $\xi < \Delta < \eta$.

In these notes we will describe Davenport-Heilbronn's proof [2] of the following result:

Theorem 1.2. [2]

$$\lim_{X\to\infty} \frac{1}{X} N_3(0, X) = \frac{1}{12\zeta(3)},$$
$$\lim_{X\to\infty} \frac{1}{X} N_3(-X, 0) = \frac{1}{4\zeta(3)}.$$

They prove their result through the following theorem:

Theorem 1.3. *There exists a bijection between triplets of conjugate cubic fields K, and a subset U of the $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms.*

This bijection preserves: (1) the discriminant, and (2) the factorization type of each prime p (i.e., the factorization type of a prime p in $K/\mathbb{Q}$ is the same as the factorization of the associated cubic form over $\mathbb{F}_p$).

Moreover, the bijection is given explicitly as follows. For a cubic field K, we let $1, \omega, \nu$ denote an integral basis, and let Δ_K denote the absolute discriminant. Then,

$$F_K(x, y) := \Delta_K^{-1/2} \Delta^{1/2}(\omega x + \nu y) \tag{1.1}$$

is the associated cubic form.

The subset U is defined by a set of local conditions for each prime p, and is to be described later.

The result then follows from the following result (copy-and-pasted from Proposition 5.1):

Theorem 1.4.

$$\lim_{X\to\infty} \frac{1}{X} N(0, X; U) = \frac{1}{12\zeta(3)},$$
$$\lim_{X\to\infty} \frac{1}{X} N(-X, 0; U) = \frac{1}{4\zeta(3)}.$$

2000 *Mathematics Subject Classification.* 11N25, 11N36.

The structure of these notes follows that of [2]. In Section 2 we (and DH) introduce some notation and definitions (and postpone the motivation for later). In Section 3 we compute some 'local densities': the densities of forms in various subsets U_p, V_p, etc., which will only depend on the coefficients of these forms modulo p^2. In Section 4 we prove an auxiliary proposition which will be needed later. This proposition tells us that the number of cubic forms with discriminant $< X$ and divisible by p^2 is $O(X/p^2)$. In Section 5 we go from local densities to global densities, which establishes Theorem 1.4. In Section 6 we prove the correspondence in Theorem 1.3, although a substantial subset (proved earlier in [1]) will be assumed.) In Section 7 we present an application to 3-torsion in quadratic fields, although the proof looked unfortunately a bit *deus ex machina* to the present author. We will conclude (at least I intend to write something eventually...) in Section 8 with an overview of Davenport and Heilbronn's earlier paper [1].

2. Notation and definitions

Definition of Φ: Φ will denote the set of all irreducible primitive binary cubic forms

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

with integer coefficients. The **discriminant** of such a form is defined to be the same as the discriminant of the associated polynomial

$$ax^3 + bx^2 + cx + d,$$

which one may check (or look up) to be

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

Equivalence: We will say that two forms $F(x,y)$ and $F(x',y')$ are **equivalent** if there exists a matrix $M \in \mathrm{GL}_2(\mathbb{Z})$ so that $(x',y') := M(x,y)$ transforms F' into F. Trivially, two equivalent forms represent the same integers.

It is a fact that **equivalence preserves the discriminant**; to give one proof, write out a change of variables and do the computation. If Brian Conrad is listening to this talk, he might begin gagging here and interrupt me to offer a more highbrow proof.

For **quadratic forms** we insist instead that $M \in \mathrm{SL}_2(\mathbb{Z})$.

We say that two forms are **rationally equivalent** if there is a nonsingular matrix M with integer entries taking F to $\delta F'$, for any rational number δ. This can easily be checked (although it is not totally immediate) that this is an equivalence relation.

Remark. It would be interesting to re-read Burton Jones's book and recall why we care about this.

Congruences: We will define two notions of congruences. We write $F_1(x,y) \equiv F_2(x,y) (\mathrm{Mod} m)$ if all the coefficients are congruent mod m. We will write $F_1(x,y) \equiv F_2(x,y) (\mathrm{mod}\ m)$ if for each pair $x, y \in \mathbb{Z}$ the forms assume values congruent to each other mod m.

Remark. It naturally occurs to me to wonder how much stronger the first condition is. Presumably D-H discuss this later.

Factorization mod p: We define a symbol (F,p) for each p depending on how the form F factors mod p. In particular, (F,p) is defined to be $(111), (12), (3), (1^3), (1^21)$, where "different 1's" denote linear forms with nonconstant quotient (i.e. which are really distinct)

We define $T_p(111), T_p(12)$, etc. to be the subsets of Φ consisting of forms which factorize in a given way mod p.

Lemma 2.1. *We have $p|D$ if any only if $(F,p) = (1^3)$ or $(F,p) = (1^21)$, and furthermore $p^2|D$ if $(F,p) = (1^3)$.*

Proof. Omitted by DH. Is this the sort of thing one should morally know? □

Definition of W_p, V_p, U_p, V, U. We say that $F \in W_p$ if $p^2|D$. (So, $T_p(1^3) \subseteq W_p$.)

We define V_p to be the complement of W_p for all $p \neq 2$. If $p = 2$ (I hate 2), we say that $F \in V_2$ if $D \equiv 1 \mod 4$ or $D \equiv 8, 12 \mod 16$. (**why??**)

We define $U_p \supseteq V_p$ to contain any $F \in U_p$, and also to contain any F with $(F, p) = (1^3)$ and if the congruence $F(x, y) \equiv ep \pmod{p^2}$ has a solution for any $e \not\equiv 0 \mod p$. In other words, U_p contains all forms where p^2 does not divide the discriminant D, and a few forms where p^2 does divide the discriminant.

Definition of U, V: We define U and V to be the intersection of U_p, V_p for all primes p.

By the definitions, we check (not too difficult) that V_p, U_p, V, U consist of complete classes of equivalent forms.

Remark. The definitions of U_p and U are motivated by what comes later; in particular, we want to define a bijection between classes in U and cubic fields up to conjugation. One should notice that U is a suitably meaty subset of Φ; the density of U in Φ will be positive and given by a convergent Euler product over all primes.

If S is any subset of Φ consisting of complete equivalence classes, we denote by $N(\xi, \eta; S)$ the number of classes in S whose forms have a discriminant $D \in [\xi, \eta]$.

Quadratic forms: We let $h_3^*(\Delta_2)$ denote the number of classes of primitive quadratic forms of discriminant Δ_2 whose cube is the unit class. (In other words, we're counting 3-torsion in the class group.)

3. Local densities

Modulo p^r, where $r = 1$ or 2, there are $p^{4r}(1 - p^{-4})$ forms over $\mathbb{Z}/p^r\mathbb{Z}$. If S is any set of forms in Φ, we let $A(S, p^r)$ denote the number of residue classes mod p^r occupied by forms in S, divided by $p^{4r}(1 - p^{-4})$.

Lemma 3.1.

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

$$A(T_p(12); p^r) = \frac{1}{2}p(p-1)(p^2+1)^{-1},$$

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

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

$$A(T_p(1^21); p^r) = p(p^2+1)^{-1}.$$

The proof is pretty easy, you just count.

Definition 3.2. *$S_1 = S_{1,p}$ denotes the set of forms $F \in \Phi$ for which $p \nmid a, p|b, p|c, p^2|d$. $S_2 = S_{2,p}$ denotes the set of forms for which $p \nmid b, p|a, p|c, p^2 d$.*

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

Lemma 3.3. *If $F \in \Sigma_1$, then $(F, p) = (1^3)$; if $F \in \Sigma_2$ then $(F, p) = (1^21)$.*

Proof. DH don't give a proof, but it looks important!!! **Figure it out.** □

Lemma 3.4 (Lemma 2)**.** *We have*

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

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

Proof. We start with the first formula. We (easily) compute that

$$A(S_1; p^2) = A(S_2; p^2) = p^{-1}(p+1)^{-1}(p^2+1)^{-1}. \tag{3.1}$$

If $M = \begin{pmatrix} k & l \\ m & n \end{pmatrix}$ is a matrix mod p^2 of determinant ± 1, we verify (by a short explicit computation) that for $F \in S_1$, $M \cdot F \in S_1$ if and only if $p|l$.

The unimodular substitutions mod p^2 with $p|l$ form a subgroup of index $p+1$ (**check it?**) of the group of all unimodular substitutions mod p^2, so if a form is in Σ_1 then there is a $1/p+1$ chance it is in S_1. The first part of the lemma now follows from 3.1.

For S_2 and Σ_2 the argument is similar. We check (in about eight lines) that for $F \in S_1$, $M \cdot F \in S_1$ if and only if $p \div l, m$. The index of this subgroup is $p(p+1)$, and the rest of the lemma follows. □

Lemma 3.5 (3)**.** *We have the disjoint union*

$$\Phi = V_p \cup T_p(1^3) \cup \Sigma_2.$$

Proof. As can be checked by some definition chasing, each F with $(F, p) \neq (1^2 1)$ belongs to one and only one of these sets. So we only need to worry about $F \in T(1^2 1)$. We may assume (**why??**) that such a form has coefficients a, b, c, d so that p divides a, c, d and not b. Then, we calculate that

$$D \equiv -4b^3 d \mod p^2.$$

For $p \neq 2$, D is divisible by p^2 if and only if d is. By our definitions, this means that F is in either V_p or Σ_2.

If $p = 2$... (never mind for now.) □

Lemma 3.6 (4, 5)**.** *We have*

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

$$A(U_p; p^2) = (p^3-1)p^{-1}(p^2+1)^{-1}.$$

Proof. The principle, anyway, is clear. We've computed enough local densities, and now we use the explicit decomposition given in Lemma 3. □

Lemma 3.7 (6)**.** *If $(F, p) = (1^3)$, then $F \in U_p$ is and only if $D \equiv 0 (\mathrm{mod}\ p^3)$. For $p = 3$, a similar condition holds.*

Proof. The proof is similar to that of Lemma 3, and is confusing for the same reason. It seems we can make some assumptions on the p-divisibility of the coefficients of F. I don't understand where they come from.

Notice that the reason for treating $p = 3$ separately is that the number 27 occurs in the discriminant. □

4. An auxiliary proposition

We define $N(-X, X; W_p)$ to be the number of equivalence classes of (cubic) forms with discriminant in $[-X, X]$ in W_p - i.e., with $p^2|D$.

It was previously proved that

$$N(-X, X) = O(X).$$

The object of this section is to prove the following extension of this result:

Proposition 4.1 (1). *We have*

$$N(-X, X; p^2) = O(Xp^{-2}).$$

Note: In the interests of time, this section has been left sketchy. There are a lot of details in the paper which I did not read especially closely, and I just left what notes I took. If you believe this proposition, you can skip to the next section.

DH first state the following lemma, which follows from **to be described**.

Lemma 4.2 (7). *We have*

$$\sum_{|Delta_2|<X} h_3^*(\Delta_2) = O(X),$$

where Δ_2 runs through the discriminants of quadratic fields.

Definition 4.3. *The* **Hessian** $H(x, y)$ *of a cubic form* $H(x, y)$ *is defined by the equation*

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

It is well known that $H(x, y)$ is a covariant of $F(x, y)$ with respect to linear substitutions of determinant 1. (**I assume** that this means that if M is some such transformation, then $H(F) = H(MF)$. This could, and should, be verified by a simple explicit calculation...)

We can calculate some more, and we get

$$H(x, y) = Px^2 + Qxy + Ry^2,$$

where $P = b^2 - 3ac, Q = bc - 9ad, R = c^2 - 3bd$. We also compute that the discriminant is given by

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

(That's really simple!! Nice!)

The class of H is uniquely determined by the class of F, but the converse is not necessarily true. The formula above shows that H is reducible if and only if the discriminant $-3D$ is a square.

We have that H is **primitive** if and only if for all primes p, $(F, p) \neq (1^3)$. (**to do: prove me**) We write $M = (P, Q, R)$, and $P = MP_1, Q = MQ_1, R = MR_1$, and

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

and this quadratic form has discrimimant $-3D/M^2$.

We can easily write down (**although, I'm still confused as to why we want to**) identities

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

$$H_1(c, -b) = MP_1R_1,$$

$$H_1(3d, -c) = MR_1^2.$$

Lemma 4.4 (8)**.** *Let k and M be positive integers, and let $B = B(k, M)$ denote the number of classes of forms in Φ with Hessian $H(x, y) = M(kx + ly)y$, where $0 \leq l < k, (l, k) = 1$. Then*

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

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

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

Remark. $\tau(M)$ denotes the number of divisors of M.

Proof. About 3/4 of a page of elementary hacking around... write down the proof? □

There is some more stuff in Section 4... which I have omitted. In brief, we have a map from cubic to quadratic forms, and we bound the size of the fibers of the map.

5. Global densities

The purpose of this section is to prove the following

Proposition 5.1. *[2, p.415]*

$$\lim_{X\to\infty} \frac{1}{X} N(0, X; U) = \frac{1}{12\zeta(3)},$$

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

The main theorem then follows from this proposition, combined with the correspondence theorem. Let $N(0, X; U)$ denote the number of equivalence classes in U with discriminant in $[0, X]$.

To prove this, we need to refer to earlier (1951) work of Davenport. He proved that

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

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

In other words, he proved asymptotics for the number of equivalence classes of binary cubic forms with discriminants in the ranges specified.

Remark. I wonder about the extent to which similar formulas can be proved for n-ary forms for general n?

In fact, we need the following extension of this result, which DH claim is proved in exactly the same way:

Proposition 5.2. *Let S_m be a set of forms in ϕ defined by conditions on the residue classes of a, b, c, d mod m. Moreover, assume that S_m is a union of* **equivalence classes** *in Φ. Then,*

$$N(0, X; S_m) \sim \frac{5}{4\pi^2} A(S_m; m) X,$$

$$N(-X, 0; S_m) \sim \frac{15}{4\pi^2} A(S_m; m) X.$$

In other words, if we restrict the coefficieints mod m, then we have the “right” factor in the asymptotic. DH remark that the result is not uniform in m.

We now can embark upon the proof of Proposition 2. To prove the first assertion, denote

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

Recall that $U := \cap_p U_p$. Recall that whether a form is in U_p or not depends only on the coefficients mod p^2, and it therefore follows that

$$\frac{1}{X} N(X, 0; \cap_{p<Y} U_p) \to \frac{5}{4\pi^2} A(\cap_{p<Y} U_p; P_Y^2).$$

In other words, the proportion of forms in $\cap U_p$ is given by a density.

We have

$$\frac{5}{4\pi^2} A(\cap_{p<Y} U_p; P_Y^2) = \frac{5}{4\pi^2} \prod_{p<Y} A(U_p; p^2) = \frac{5}{4\pi^2} \prod_{p<Y} (p^2-1)p^{-1}(p^2+1)^{-1},$$

where the last step follows from our earlier computation of local densities.

We therefore conclude that

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

This is true for each Y, so we can replace the finite product with an infinite one. We get on the right

$$\frac{5}{4\pi^2} \prod_p (1-p^{-3})(1+p^{-2})^{-1} = \frac{5\zeta(4)}{\zeta(2)\zeta(3)\pi^2} = \frac{1}{12\zeta(3)}.$$

We now prove that the liminf is the same thing, by observing that

$$\cap_{p<Y} U_p \subseteq (U \cup \cup_{p\leq Y} W_p).$$

Thus,

$$\frac{5}{4\pi^2} \prod_{p<Y} (p^2-1)p^{-1}(p^2+1)^{-1} \leq \liminf_{X\to\infty} (\frac{1}{X} N(0, X; U) + \frac{1}{X} \sum_{p\geq Y} N(0, X, W_p)).$$

We recall that $\frac{1}{X} N(0, X; W_p) = O(p^{-2})$, so the second sum is $o_Y(1)$, and letting Y tend to infinity, we see the liminf and the limsup are the same.

Remark. They prove similar results with V in place of U. (Perhaps we will decide that we care...?)

6. The Fundamental Mapping

In this section we will discuss DH's proof of the fundamental mapping (given previously). We recall that the mapping is given by

$$F_K(x, y) := \Delta_K^{-1/2} \Delta^{1/2}(\omega x + \nu y), \tag{6.1}$$

where $1, \omega, \nu$ is an integral basis of K, and that this mapping preserves (1) the discriminant and (2) the factorization type. of each prime p (i.e., the factorization type of a prime p in $K/\mathbb{Q}$ is the same as the factorization of the associated cubic form over $\mathbb{F}_p$).

DH first prove that the factorization type is preserved. (It looks mostly like a triviality, once the appropriate appeal to algebraic number theory has been made. **But...** that polynomial is not quite what I was expecting.)

Lemma 6.1 (12, p. 416)**.** *For any K, F_K is in U.*

Proof. Naturally we check it for each p. The cases $p = 2$ and $p = 3$ provoke an ugly mess which I will ignore for the time being.

We will recall some 'well-known' facts on cubic fields. If K is cyclic, then its discriminant Δ_K is a square (proof: $\sqrt{\Delta_K} \in K$.) If K is not cyclic, then we can write $\Delta_K = \Delta_2 f^2$, where Δ_2 is the discriminant of a quadratic field. In both cases $p^2 \nmid f$ is $p \neq 3$, and $(\Delta_2, f) = 1$ or 3. Also, if $p \neq 2$, then $p^2 | \Delta^2$. (Certainly.) A prime p ramifies completely in K if and only if $p|f$. (Interesting...)

Now, to show that $F_K \in U_p$ for all p. If $p^2 \nmid \Delta_K$, this follows immediately from the definition.

If $p^2 | \Delta_K$, and $p > 3$, then we know that $p|f$, and p ramifies completely in K. By Lemma 11, we have $(F_K, p^3) = (1^3)$. As $p^3 \nmid \Delta_K$, Lemma 6 implies that $F_K \in U_p$. □

Remark. We used the fact that $p \neq 3$ in citing Lemma 6, and I presume that a cubic field can have discriminant divisible by 8? (**check it...**)

Lemma 6.2 (13)**.** *For forms in U, rational equivalence is the same as equivalence.*

Proof. A brief look at the proof convinced me this is fairly elementary, and not too difficult... write down some matrices and congruences, and the weird definition of U pops out here. Details omitted. □

Lemma 6.3 (14, p. 418)**.** *To every $F \in \Phi$ there belongs a cubic field K such that F and F_K are rationally equivalent.*

Proof. The proof is kind of nice. Factor F as

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

and λ generates a cubic field K.

Now, go the other way and look at F_K. Write it

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

If K is not cyclic, μ is unique, but if K is cyclic then any of the three conjugates can be used. (**to do: prove those claims.**) Now μ and λ are both irrationals in K, so $1, \mu, \lambda, \mu\lambda$ have a linear dependence relation, which we may write as

$$\mu = \frac{k\lambda + l}{m\lambda + n},$$

where $(k, l, m, n) = 1$, and the above is unique (up to multiplying k, l, m, n by -1.)

We then check (**do it**) that the transformation

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

transforms F into a constant multiple of F_K. □

So the punchline is clear, right? If $F \in U$, then we can delete the adjective 'rationally', and we have our bijection. Done.

7. 3-torsion in quadratic fields

We can prove the following too. Let $h_3^*(\Delta_2)$ denote the number of elements $\alpha \in \mathrm{Cl}(\mathbb{Q}(\sqrt{\Delta_2}))$ with $\alpha^3 = 1$.

Theorem 7.1 (Theorem 3, p. 406)**.** *We have*

$$\sum_{0<\Delta_2<X} h_3^*(\Delta_2) \sim \frac{4}{3} \sum_{0<\Delta_2<X} 1,$$

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

Proof. Let K be a cubic field in which no prime ramifies completely. This implies that K is not cyclic, and that Δ_K is the discriminant of a quadratic field. A theorem of Hasse says that for a given Δ_K, the number of triplets of such cubic fields equals

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

But, these fields are in 1-1 correspondence with the classes of cubic forms in V. Thus,

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

We know what to do from here. □

8. Davenport-Heilbronn's earlier work on the fundamental mapping

Recall, again, that we have defined a mapping from cubic fields to binary cubic forms by

$$F_K(x,y) := \Delta_K^{-1/2} \Delta^{1/2}(\omega x + \theta y), \tag{8.1}$$

where $1, \omega, \theta$ is an integral basis of K. The first portion of [1] is devoted to proofs of the following results:

Lemma 8.1. *$F_K(x,y)$ has coefficients in $\mathbb{Z}$.*

Proof. We factor $F_k(x,y)$ in its Galois closure K as

$$F_l(x,y) = d^{-1/2}\Big((\omega - \omega')x + (\theta - \theta')y\Big)\Big((\omega' - \omega'')x + (\theta' - \theta'')y\Big)\Big((\omega'' - \omega)x + (\theta'' - \theta)y\Big),$$

where we choose an arbitrary but fixed sign for $d^{-1/2}$.

The coefficient of x^3 is $d^{-1/2}\mathfrak{d}^{1/2}(\omega)$, which lies in $\mathbb{Z}$ as ω is an algebraic integer. We may write $\theta = (\omega^2 + a\omega + b)/c$, where the discriminant of ω is dc^2 (there is an exercise in algebraic number theory to do here...)

We compute that the coefficient of x^2y is

$$d^{-1/2}\mathfrak{d}^{1/2}(\omega)\left(\frac{\theta-\theta'}{\omega-\omega'} + \frac{\theta'-\theta''}{\omega'-\omega''} + \frac{\theta''-\theta}{\omega''-\omega}\right),$$

and we check that this equals

$$d^{-1/2}\mathfrak{d}^{1/2}(\omega)c^{-1}\mathrm{Tr}_{k/\mathbb{Q}}(2\omega + a) = \mathrm{Tr}_{k/\mathbb{Q}}(2\omega + a),$$

which is an integer. The conclusion follows by symmetry. □

Lemma 8.2. *$F_K(x,y)$ is irreducible over $\mathbb{Q}$.*

Proof. If it were reducible, then we could find $x_0, y_0 \in \mathbb{Q}$ so that $F_k(x_0, y_0) = 0$. This would imply that the discriminant of $x_0\omega + y_0\theta$ was zero. But this cannot happen (**presumably this is easy algebraic number theory?**) because $x_0\omega + y_0\theta \notin \mathbb{Q}$. □

Lemma 8.3. *$F_K(x,y)$ has discriminant d.*

Proof. (to be added) □

Lemma 8.4. *$F_k(x,y)$ is primitive – the coefficients are coprime.*

Proof. Appeal to a 1930 paper of Hasse (wer auf Deutsch ist). □

Lemma 8.5. *If k_1 is a cubic field not conjugate to k, then the forms $F_k(x, y)$ and $F_{k_1}(x, y)$ are not equivalent.*

Proof. The zeroes of the polynomial $F_k(x, 1)$ lie in the Galois closure K of k. But if k_1 is not conjugate to k, then K does not contain k_1. □

References

[1] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields*, Bull. London Math. Soc. 1 (1969), 345-348.

[2] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. Lond. A. 322 (1971), 405-420.

Department of Mathematics, Stanford University
E-mail address: fthorne@math.stanford.edu