Hardy-Ramanujan Journal
Vol.29 (2006) 1-17

On polynomials that equal binary cubic forms

C. HOOLEY

1. Introduction

There has been a long standing expectation that, if $F(x_0, \ldots, x_r)$ be a polynomial with rational integral coefficients that assumes numerical values of a certain shape for all integral $x_0, \ldots, x_r$ (or at least for all sufficiently large values thereof), then it is actually identically of this shape in appropriate circumstances. In a recent publication [2], to which we refer the reader for some history of the matter and for our mention of Schinzel's work [4], we proved that this expectation was indeed fulfilled when $F(x_0, \ldots, x_r)$ is a cubic that is always equal to a sum of two cubes when $x_0, \ldots, x_r$ are integers. In the knowledge that we would later reduce the proposition by an algebraic process to the most interesting case where $r = 0$, we began with a polynomial $F(x)$ and considered the two situations where it was assumed that $F(n)$ for all large n was either (i) a sum of two *positive* cubes or (ii) merely a sum of two cubes of either sign. In each case a successful conclusion was reached, even to the extent that we were ultimately supplied with a parametric representation of $F(n)$ that yielded a decomposition of the precise type postulated.

It is now natural to ask how the enquiry is affected by our changing the requirement on the cubic polynomial $F(x)$ to one where $F(n)$ for large n is always equal to a value assumed through integers u, v by an irreducible binary cubic form

$$f(u, v) = au^3 + bu^2v + cuv^2 + dv^3$$

with rational integral coefficients. A harder problem of a different character is then seen to emerge because of the absence of the features that facilitated our solution of the original questions. In what follows we therefore seek an alternative treatment, whose pursuit leads to a complete solution in certain well defined circumstances but leads otherwise to conclusions that fall close to but definitely short of what we want. In fact, to be as precise as we can without seriously anticipating future definitions, we shall shew that there are two separate scenarios in which our hypothesis implies that $F(x)$ is identically equal to $f(u, v)$ where u, v are certain linear binomials $u(x)$, $v(x)$ with rational integral coefficients. In the first $F(x)$ and $f(u, v)$ are associated with what we call fundamental cubic forms, the nature of which will be discussed later, while in the second the greatest square factors of the discriminants of $F(x)$ and $f(u, v)$ are equal and the genus to which $f(u, v)$ belongs consists of only one class. Furthermore the result actually remains in the general situation save for the serious imperfection that the coefficients in $u(x)$, $v(x)$ are no longer necessarily integers, being either rationals or purely cubic irrationalities; in this event, integral values of n may not lead to integral values of $u(n)$ and $v(n)$ and our representation of $F(x)$ by $f(u, v)$ will not produce the one assumed in the hypothesis.

The method depends both on results from a classical realm of algebraic number theory and on certain properties of binary cubic forms that may be unfamiliar but that are easy to establish. It has therefore been both possible and desirable to provide a largely self-contained account in which most of what is needed is provided without the citation of previous work. This is particularly so in regard to fundamental forms[1], the theory of which was initiated by Levi [3], since what we need here can be supplied by a short demonstration.

2. Preliminary lemmata

We begin with some preliminary results through which we shall exploit our initial deductions from the hypothesis on $F(x)$.

First we state the familiar

LEMMA 1. *Let $\tau(p)$ be the number of incongruent zeros,* mod p, *of a given (non-constant) irreducible polynomial $g(x)$ with integral coefficients. Then, as*

[1] Inherently the index forms of Delone and Fadeev's treatise [1], which, however, treats such matters differently. We use the designation 'fundamental' because as an adjective it is better adapted for the text.

$y \to \infty$,

$$\sum_{p \le y} \rho(p) \sim \operatorname{li} y.$$

For a zero α of $g(x)$ in the field of complex numbers, let us consider the field $\mathbb{Q}(\alpha)$ and the prime ideals $\mathfrak{p}$ thereof. Then, by the prime ideal theorem,

$$\sum_{N\mathfrak{p} \le y} 1 \sim \operatorname{li} y,$$

which equivalence is still true when the ideals $\mathfrak{p}$ in the summation are restricted to be linear. But Dedekind has shewn that, for each p not dividing the (non-zero) discriminant of $g(x)$, the number of incongruent roots of the congruence $g(x) \equiv 0, \bmod p$, is equal to the number of linear ideals $\mathfrak{p}$ dividing p. The result then follows.

The form of Chebotarev's theorem we need for cubics is easily directly proved and is given by

LEMMA 2. *Let us adopt the notation of* Lemma 1 *and assume that $g(x)$ is now a cubic with discriminant D. Let also $N_i(y)$ for $i = 0, 1, 3$ denote the number of primes p not exceeding y for which $\tau(p) = i$. Then, if D be not a perfect square, namely, if $g(x)$ be non-Abelian,*

$$N_0(y) \sim \frac{1}{3} \operatorname{li} y, \qquad N_1(y) \sim \frac{1}{2} \operatorname{li} y, \qquad N_3(y) \sim \frac{1}{6} \operatorname{li} y,$$

as $y \to \infty$. But, if D be a perfect square, namely, if $g(x)$ be Abelian,

$$N_0(y) \sim \frac{2}{3} \operatorname{li} y, \qquad N_3(y) \sim \frac{1}{3} \operatorname{li} y,$$

as $y \to \infty$.

If $p \nmid D$, the value of $\rho(p)$ is 0, 1, or 3. In the intermediate case, for some integer l we have

$$g(x) \equiv (x - l) g_1(x), \bmod p,$$

in which $g_1(x)$, having no zeros, mod p, has a discriminant D_1 that is a quadratic non-residue, $\bmod p$. Since also

$$D \equiv g_1^2(l) D_1, \bmod p,$$

we see that $(D \mid p) = -1$.

In the last case, there are three incongruent integers l_1, l_2, l_3 for which

$$g(x) \equiv (x - l_1)(x - l_2)(x - l_3), \bmod p,$$

the discriminant of the right-hand polynomial being a non-zero perfect square. Hence here $(D \mid p) = 1$.

In the first case let us interpret $g(x)$ as a polynomial over the finite field $\mathbb{F}_p$ that is irreducible over this field. Then, since any finite extension of $\mathbb{F}_p$ is Abelian, the discriminant of $g(x)$ is the square of an element of $\mathbb{F}_p$ and, reverting to congruences, $\bmod p$, we find that $(D \mid p) = 1$.

Now assume first that D be not a perfect square and deduce that

$$N_1(y) \sim \sum_{\substack{p \le y \\ (D|p)=-1}} 1 \sim \frac{1}{2} \operatorname{li} y,$$

whence, by Lemma 1,

$$N_3(y) \sim \frac{1}{3} \left(\sum_{p \le y} \tau(p) - N_1(y) \right) \sim \frac{1}{6} \operatorname{li} y$$

and then

$$N_0(y) \sim \sum_{p \le y} 1 - N_1(y) - N_3(y) \sim \frac{1}{3} \operatorname{li} y.$$

But, if D be a perfect square, $\tau(p)$ is either 0 or 3 unless $p \mid D$. In this case

$$N_3(y) \sim \frac{1}{3} \sum_{p \le y} \tau(p) \sim \frac{1}{3} \operatorname{li} y$$

and

$$N_0(y) \sim \sum_{p \le y} 1 - N_3(y) \sim \frac{2}{3} \operatorname{li} y,$$

with which equivalences we complete the proof of what was asserted.

As customary, the coefficients of $\operatorname{li} x$ in these formulae are termed the densities of the categories of primes being counted.

The next lemma states a part of Chebotarev's theorem that we verify directly.

LEMMA 3. *Let us again adopt the notation of Lemma* 1 *and suppose that* $g(x)$ *is nonic. Then the number of primes* p *exceeding* y *for which* $\tau(p)$ *has its maximal possible value* 9 *is not less than*

$$c \operatorname{li} y \qquad (y > y_0).$$

Having formed the field $\mathbb{Q}(\alpha)$ as in the proof of Lemma 1, we construct the normal splitting field $\mathbb{S}$ of $g(x)$ that is degree of $d \leq 9!$ over $\mathbb{Q}$. Then over $\mathbb{S}$ a sufficiently large prime p either splits totally into d distinct linear prime ideal factors $\mathfrak{q}$ or has no such factors. Hence the number of primes p in the former category is asymptotically equivalent to

$$\frac{1}{d} \sum_{\substack{N\mathfrak{q} \leq y \\ N\mathfrak{q} \text{ linear}}} 1 \sim \frac{1}{d} \sum_{N\mathfrak{q} \leq y} 1 \sim \frac{1}{d} \operatorname{li} y. \tag{1}$$

But a sufficiently large prime splitting totally over $\mathbb{S}$ certainly splits totally over $\mathbb{Q}(\alpha)$ and therefore possesses the property that $\tau(p) = 9$, which fact with (1) substantiates the lemma.

Finally there is

LEMMA 4. *Let* $g_1(x)$, $g_2(x)$ *be irreducible polynomials with rational integral coefficients of degrees* r, s *with respective zeros* α, β. *Suppose also the degree of the field* $\mathbb{Q}(\alpha, \beta)$ *is* rs. *Then there is an irreducible polynomial* $g_3(x)$ *with rational integral coefficients with the property that, if* $\tau_i(p)$ *denote the number of incongruent zeros of* $g_i(x)$, *we have*

$$\tau_3(p) = \tau_1(p)\tau_2(p)$$

for $p > p_0$.

This can be proved by ideal theory but it is better to proceed in a more straightforward manner.

By the simplicity of algebraic extensions the field $\mathbb{Q}(\alpha, \beta)$ is the same as $\mathbb{Q}(\gamma)$ when $\gamma = \alpha + h\beta$ for some suitable rational integer h. Using the leading coefficients a_0, b_0 of $g_1(x)$ and $g_2(x)$ and the conjugates $\alpha_1, \ldots, \alpha_r$ and $\beta_1, \ldots, \beta_s$ of α and β over $\mathbb{Q}$, form the polynomial

$$g_3(x) = a_0^s b_0^r \prod_{i,j} (x - \alpha_i - h\beta_j)$$

whose coefficients are derived from symmetric functions and are therefore integers. This is irreducible because γ is a zero and its degree rs is equal to the degree of γ over $\mathbb{Q}$; in particular, its discriminant D_0 is not zero.

Let us now consider the reduction $\bar{g}_3(x)$ of $g_3(x), \bmod p$, as a polynomial over the field $\mathbb{F}_p$ of p elements. Then, if $u_1, \ldots, u_r$ and $v_1, \ldots, v_s$ be the zeros of the reductions of $g_1(x)$ and $g_2(x), \bmod p$, it is evident that

$$\bar{g}_3(x) = a_0^s b_0^r \prod_{i,j} (x - u_i - hv_j)$$

by a comparison of corresponding symmetric functions in α_i, β_j and u_i, v_j that depend on the coefficients of $g_1(x)$, $g_2(x)$ and those of the reductions $\bar{g}_1(x)$, $\bar{g}_2(x)$. Next, as $p \nmid D_0$ for $p > p_0$ and therefore $\bar{g}_3(x)$ has no repeated factors, it follows that $u_i + hv_j$ only belongs to $\mathbb{F}_p$ if u_i, $v_j \in \mathbb{F}_p$, since otherwise distinct conjugates of (u_i, v_j) over $\mathbb{F}_p$ would yield the same factor in $\bar{g}_3(x)$ more than once. Consequently, reverting to congruences, $\bmod p$, we deduce that the number of zeros, $\bmod p$, of $g_3(x)$ is equal to $\tau_1(p)\tau_2(p)$.

3. The initial consequences of the hypothesis

We are ready to state formally the property we assign to the cubic polynomials we study.

HYPOTHESIS P. $F(x)$ *is a cubic polynomial with rational integral coefficients with the property that, for all sufficiently large integers* n, $F(n)$ *is equal to a value assumed, through integers* u, v, *by a given irreducible binary cubic form*

$$f(u, v) = au^3 + bu^2v + cuv^2 + dv^3$$

with rational integral coefficients.

It is sometimes helpful to use a nomenclature to describe an association between cubic polynomials $G(x)$ and binary cubic forms $g(u, v)$. We say these are *companions* if $G(x) = g(x, 1)$ or, what is equivalent, $g(x, y) = y^3G(x/y)$; each is then said to be the *companion* of the other.

Let us denote the number of incongruent zeros, $\bmod l$, of $F(x)$ and the companion $f(x, 1)$ of $f(u, v)$ by $\rho_1(l)$ and $\rho_2(l)$, respectively. Then, if $\rho_1(p) > 0$, the number of integers n between a sufficiently large N (inclusive) and $N + p^3$ (exclusive) conforming to the conditions

$$F(n) \equiv 0, \bmod p, \qquad\qquad F(n) \not\equiv 0, \bmod p^3,$$

equals

$$p^2\rho_1(p) - \rho_1(p^3) = (p^2 - 1)\rho_1(p) > 0$$

for $p > p_0$. Hence, by Hypothesis P, for any such solution n the value of $f(u, v)$ attained by $F(n)$ is divisible by p and not p^3 and is therefore provided by integers u, v indivisible by p, since the irreducibility of $f(u, v)$ implies its leading and trailing coefficients are non-zero and thus indivisible by p for $p > p_0$. Consequently, choosing m so that $mv \equiv u, \bmod p$, we deduce that $f(m, 1) \equiv 0, \bmod p$, and $\rho_2(p) > 0$. We have thus established the simple fact that

$$\text{`}\rho_2(p) > 0 \text{ whenever } \rho_1(p) > 0 \text{ and } p > p_0\text{'}, \tag{2}$$

upon which we depend in developing our theme.

We can immediately dismiss the possibility that $F(x)$ be reducible. For in that event $F(x)$ would have a linear factor that would have a zero, modulo every sufficiently large prime p, and, by (2), we would infer that $\rho_2(p) > 0$ for $p > p_0$ in contravention of Lemma 2.

Next let θ and ϕ be zeros of $F(x)$ and $f(x, 1)$ and regard the fields $\mathbb{Q}(\theta)$ and $\mathbb{Q}(\phi)$, both of which are cubic by what has just gone before. We shall shew that these fields are isomorphic by assuming the opposite and deducing a contradiction.

On this assumption the field $\mathbb{Q}(\theta, \phi)$ is either sextic or nonic over $\mathbb{Q}$. In the former case ϕ would be quadratic over $\mathbb{Q}(\theta)$, with respect to which it would have a minimal polynomial

$$x^2 + b_1(\theta)x + c_1(\theta)$$

where $b_1(\theta)$ and $c_1(\theta)$ are (linear) polynomials in θ with rational coefficients. Then the cubic $f(x,1)$ is divisible by this quadratic, the resulting quotient being a linear polynomial

$$d_1x + e_1(\theta)$$

with rational coefficient $d_1 \neq 0$ and a coefficient $e_1(\theta)$ similar to $b_1(\theta)$, $c_1(\theta)$ above. The zero $-e_1(\theta)/d_1$ of this, being a zero of $f(x,1)$, is a conjugate of ϕ and $\mathbb{Q}(\theta)$ and $\mathbb{Q}(\phi)$ would be isomorphic; the first case therefore cannot occur.

We must thus suppose that $\mathbb{Q}(\theta,\phi)$ is nonic and that $F(x)$, $f(x,1)$are examples of the polynomials $g_1(x)$, $g_2(x)$ occurring in the statement of Lemma 4, in which $\tau_1(p) = \rho_1(p)$, $\tau_2(p) = \rho_2(p)$, and $\rho(p) = \rho_1(p)\rho_2(p)$ is the number of incongruent zeros, mod p, of an irreducible nonic polynomial with integral coefficients. We then consider separately the following four possible cases in the light of principle 2:

(i) $\mathbb{Q}(\theta)$ non-Abelian, $\mathbb{Q}(\phi)$ Abelian,

(ii) $\mathbb{Q}(\theta)$ Abelian, $\mathbb{Q}(\phi)$ Abelian,

(iii) $\mathbb{Q}(\theta)$ Abelian, $\mathbb{Q}(\phi)$ non-Abelian,

(iv) $\mathbb{Q}(\theta)$ non-Abelian, $\mathbb{Q}(\phi)$ non-Abelian.

The first case can be rejected at once, since by Lemma 2 the density of primes for which $\rho_1(p) > 0$ exceeds that for which $\rho_2(p) > 0$.

In the second case the primes $p > p_0$ for which $\rho_1(p) > 0$ are precisely those for which $\rho_1(p)$ and $\rho_2(p)$ are non-zero and for which, therefore, $\rho(p) = 9$. Hence, by Lemma 1, the cardinality of these primes that do not exceed y is asymptotic to

$$\frac{1}{9}\sum_{p\leq y}\rho(p) \sim \frac{1}{9}\operatorname{li} y,$$

whereas it is $\frac{1}{3}\operatorname{li} y$, by Lemma 2; the second case is thus eliminated.

In the third case, if $\rho_1(p) > 0$, then $\rho_1(p) = 3$ and $\rho_2(p) = 3$ or 1. When $\rho_2(p) = 3$ here, $\rho(p)$ assumes its maximal value 9 for $n(y)$ primes p between p_0 and y, where Lemma 3 states that

$$n(y) > c \operatorname{li} y,$$

for some small constant c. Thence the number of primes p up to y for which $\rho_1(p) > 0$ is asymptotic to

$$\begin{aligned}
\frac{1}{3}\sum_{\substack{p\le y\\ \rho(p)=3}} \rho(p) + n(y) &= \frac{1}{3}\left\{\sum_{p\le y}\rho(p) - 9n(y)\right\} + n(y)\\
&= \frac{1}{3}\sum_{p\le y}\rho(p) - 2n(y)\\
&< \frac{1}{3}(1-c)\operatorname{li} y \qquad (y > y_0)
\end{aligned}$$

in violation of Lemma 2, this case being also impossible.

The demonstration in the fourth case is made more transparent if we cite the obvious

LEMMA 5. *Let $\lambda_1, \dots, \lambda_r$; $\mu_1, \dots, \mu_r$ be two non-decreasing sequences of positive numbers. Then no sum of the type*

$$\lambda_1\mu_{i_1} + \cdots + \lambda_r\mu_{i_r}$$

for any permutation $i_1, \dots, i_r$ of $1, \dots, r$ is less than

$$\lambda_1\mu_r + \cdots + \lambda_r\mu_1.$$

The number of p up to y for which $\rho_1(p) = 1$ or 3 is asymptotically equivalent to $\frac{1}{2}\operatorname{li} y$ or $\frac{1}{6}\operatorname{li} y$ by Lemma 2; the same being true for $\rho_2(p)$ without restriction of $\rho_1(p)$, by (2) it is still true when $\rho_1(p)$ is confined to non-zero values. Hence, glancing at Lemma 5, we would deduce that

$$\begin{aligned}
\sum_{p\le y}\rho(p) &\sim \sum_{p\le y}\rho_1(p)\rho_2(p)\\
&> 3\left(\frac{1}{6}-\varepsilon\right)\operatorname{li} y + 3\left(\frac{1}{6}-\varepsilon\right)\operatorname{li} y + \left(\frac{1}{3}-\varepsilon\right)\operatorname{li} y\\
&> \frac{4}{3}(1-7\varepsilon)\operatorname{li} y \qquad (y > y_0)
\end{aligned}$$

in opposition to Lemma 1.

We have therefore proved that the fields $\mathbb{Q}(\theta)$ and $\mathbb{Q}(\phi)$ are isomorphic; indeed we see that they are same provided that ϕ be chosen, as it usually will be, to be a suitable zero of $f(x,1)$. From this fact we proceed to the first relationship between $F(x)$ and $f(u,v)$ by confirming the known consequence that θ and ϕ are subject to an homography.

All polynomials in this paragraph having rational coefficients, we have

$$\phi = g(\theta) = a_2\theta^2 + b_2\theta + c_2.$$

If $a_2 \neq 0$, then by the division algorithm there are linear polynomials $l_1(x)$, $l_2(x)$ such that

$$f(x,1) = l_1(x)g(x) - l_2(x)$$

identically, whence

$$l_1(\theta)g(\theta) - l_2(\theta) = 0$$

and

$$\phi = \frac{l_2(\theta)}{l_1(\theta)} = \frac{A\theta + B}{C\theta + D} \tag{3}$$

for integers A, B, C, D on which may be imposed the condition

$$(A,B,C,D) = 1 \tag{4}$$

in addition to the necessary

$$AD - BC \neq 0. \tag{5}$$

If, however, $a_2 = 0$, then $b_2 \neq 0$ and we already have (3) with a value of C that is zero.

Since the homography (3) implies that

$$f(A\theta + B, C\theta + D) = 0,$$

we infer that the polynomials $F(x)$ and $f(Ax+B, Cx+D)$ are proportional in the sense that

$$k_1F(x) = k_2f(Ax+B, Cx+D) \tag{6}$$

for coprime integers k_1, k_2 that may be both taken to be positive by changing the signs of A, B, C, D if necessary. Alternatively, if $\mathrm{F}(x,y)$ denote the companion of $F(x)$, this may be stated as

$$k_1\mathrm{F}(x,y) = k_2f(Ax+By, Cx+Dy) \tag{7}$$

when we wish to work in the language of forms and linear substitutions. Hence, setting $k_3 = \sqrt[3]{k_2/k_1}$, we deduce that

$$F(x) = f(Ak_3x + Bk_3, Ck_3x + Dk_3)$$

and shew that

'*on* Hypothesis P, *the polynomial $F(x)$ is identically equal to $f(u, v)$ when $u = u(x)$, $v = v(x)$ are certain linear binomials in x*'.

This, however, does not achieve all we seek because integer values of n do not necessarily supply the integer values of u and v that correspond to the representation of $F(n)$ postulated by Hypothesis P.

Being currently unable to achieve more on Hypothesis P alone, we therefore go on to see whether what we desire can be obtained by augmenting our assumption with some side conditions. These are associated with the concepts of fundamental (cubic) form and genus, which are the subject of the next Section.

4. Fundamental forms and genera

We describe a treatment of a bi-unique correspondence between certain binary cubic forms and cubic fields that was constructed by Levi [3] in 1914. In this account two forms are said to be *equivalent* if they be derived from each other through (unimodular) substitutions having integer coefficients and determinant ±1, all forms equivalent to each other constituting a *class*. One side of the correspondence consists of primitive irreducible cubic forms $\phi(x, y)$ — named by us *fundamental* for convenience[2] — that do not have the property that there is some non-zero integer k other than ±1 for which $k\phi(x, y)$ arises from a form $\Phi(x, y)$ with integral coefficients through a substitution of determinant k. Since two cubic forms that are equal save for sign are equivalent, it is clear that a form equivalent to a fundamental form is also fundamental and that we may therefore employ the term *fundamental class*. Also, if $\phi(x, y)$ be not fundamental and have discriminant D_1, the form $\Phi(x, y)$ from which it arises through an integer k of size exceeding 1 has a discriminant D_2 given by $k^4 D_1 = k^6 D_2$ and therefore by

$$D_2 = \frac{1}{k^2} D_1. \tag{8}$$

[2] See footnote 1).

By what has been done towards the end of the previous Section it is plain that to each cubic field (regarding all conjugate fields as the same) there is associated bi-uniquely a set $\mathcal{S}$ of integral cubic forms of the type

$$l\psi(Ax+By, Cx+Dy), \tag{9}$$

where l is rational, (4) and (5) hold, and where the choice of the particular form $l\psi(u,v)$ within $\mathcal{S}$ is irrelevant. All forms in $\mathcal{S}$ have non-zero discriminant of the same sign; let us therefore choose one of them (or the class containing it) that possesses a discriminant of minimum size. This by (8) is fundamental and $\mathcal{S}$ contains at least one fundamental class. This class is unique, as we now shall shew.

Suppose the forms $g_1(x,y)$ and $g_2(x,y)$ in $\mathcal{S}$ are both fundamental and deduce first from (9) and primitivity that

$$g_1(x,y) = \frac{1}{E_1} g_2(Ax+By, Cx+Dy), \tag{10}$$

where $(A,B,C,D) = 1$, $AD - BC = M \neq 0$, and E_1 is a non-zero integer. This we treat by finding unimodular matrices $\mathbf{P}$, $\mathbf{Q}$ with integral elements that are to appear in the equation

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \mathbf{P} \begin{bmatrix} 1 & 0 \\ 0 & |M| \end{bmatrix} \mathbf{Q},$$

whence, transforming $g_1(x,y)$, $g_2(x,y)$ into equivalent forms $h_1(X,Y)$, $h_2(X,Y)$ by the substitutions represented by $\mathbf{Q}$, $\mathbf{P}$, respectively, we deduce that

$$h_1(X,Y) = \frac{1}{E_1} h_2(X, |M|Y). \tag{11}$$

Also, setting $X = |M|X'$, $Y = |M|Y'$, and then suppressing the notational primes, we have the parallel identity

$$h_2(X,Y) = \frac{E_1}{|M|^3} h_1(|M|X, Y) = \frac{1}{E_2} h_1(|M|X, Y), \tag{12}$$

where E_2 is an integer by primitivity and $E_1 E_2 = |M|^3$.

Assume that $|M| > 1$. Then, for some prime p, we have $p^a \| M$, $p^b \| E_1$, $p^c \| E_2$, where $b + c = 3a > 0$ and thus where either

$$b < 2a \qquad \text{or} \qquad c < 2a. \tag{13}$$

In the former instance, letting $E_1 = {E_1}'p^b$, $|M| = M'p^a$, we see that the right side of (11) equals

$$\frac{1}{p^b {E_1}'} h_2(X, p^a M'Y) = \frac{1}{p^b} h_3(X, p^a Y),$$

in which the form

$$h_3(\xi, \eta) = a_3\xi^3 + b_3\xi^2\eta + c_3\xi\eta^2 + d_3\eta^3$$

has integral coefficients. Since

$$\begin{aligned} h_1(X,Y) &= a_3p^{-b}X^3 + b_3p^{a-b}X^2Y + c_3p^{2a-b}XY^2 + d_3p^{3a-b}Y^3 \\ &= {a_3}'X^3 + {b_3}'X^2Y + c_3p^{2a-b}XY^2 + d_3p^{3a-b}Y^3 \end{aligned}$$

with integral ${a_3}'$, ${b_3}'$, it follows that

$$\begin{aligned} ph_1(X,Y) &= {a_3}'pX^3 + {b_3}'X^2(pY) + c_3p^{2a-b-1}X(pY)^2 + d_3p^{3a-b-2}(pY)^3 \\ &= h_4(X, pY) \end{aligned}$$

and that $h_1(X,Y)$ would not be fundamental. Since the other case $c < 2a$ in (13) can be treated similarly by (12) to reach the false conclusion that $h_2(X,Y)$ would not be fundamental, we conclude that $|M| = |E_1| = 1$ in (10) and that $g_1(x,y)$ and $g_2(x,y)$ are equivalent through the equivalence of $h_1(X,Y)$ and $h_2(X,Y)$.

We have thus confirmed the verity of Levi's bi-unique correspondence between (classes of) fundamental cubic forms and cubic fields. To complete our preparations for our final results there are now attached some comments about genera of cubic forms and their connection with fundamental forms.

Two primitive cubic forms are said to belong to the same (primitive) *genus* if either can be transferred into the other by means of a unimodular substitution with rational coefficients; a genus is divided into a number of complete classes. It is simple to shew that a primitive cubic form belonging to a genus containing more than one class is not fundamental. For suppose that $f_1(x,y)$ is such a form so that there is a primitive inequivalent form $f_2(x,y)$ satisfying an identity

$$f_1(x,y) = f_2(\alpha'x + \beta'y, \gamma'x + \delta'y), \tag{14}$$

wherein α', β', γ', δ' are rationals that appear in the equation $\alpha'\delta' - \beta'\gamma' = \pm 1$. Multiply α', β', γ', δ' by a positive integer r, necessarily greater than 1, to obtain integers A, B, C, D that conform to the conditions

$$(A, B, C, D) = 1, \qquad AD - BC = \pm r^2, \tag{15}$$

the outcome being a relation of type (11) with $E_1 = r^3$ and $M = \pm r^2$. If it be analyzed as previously, then $a = 2$, $b = 3$, and $b < 2a$, and we infer that $f_1(x, y)$ is not fundamental.

Lest our final theorem seem otiose, we must shew that the converse of the above preposition is false, namely, that there are non-fundamental forms that belong to genera containing only one class. Choose any odd prime p that is congruent to 2, mod 9, and take the form $x^3 + p^2y^3$, which is not fundamental because its product with p is derived from $px^3 + y^3$ by a substitution of determinant p. If it belonged to a genus of more than one class, there would be a form $f_2(x, y)$ to which it is related through an identity

$$x^3 + p^2y^3 = \frac{1}{r^3} f_2(Ax + By, Cx + Dy) \qquad (|r| > 1)$$

as in (14) and (15). Then, by previous reasoning, this becomes

$$\begin{aligned} (\alpha X + \beta Y)^3 + p^2(\gamma X + \delta Y)^3 &= \frac{1}{r^3} h_2(X, r^2Y) \\ &= a_4X^3 + b_4X^2Y + c_4rXY^2 + d_4r^3Y^3, \text{ say,} \end{aligned}$$

where α, β, γ, δ are integers satisfying $\alpha\delta - \beta\gamma = \pm 1$, the first inference being

$$\beta^3 + p^2\delta^3 \equiv 0, \bmod r^3. \tag{16}$$

Since $(\beta, \delta) = 1$ and $-p^2 \equiv 5 \bmod 9$, is not a cubic residue, mod 9, we see that $3 \nmid r$; also, if $p \mid r$, then $p \mid \beta$ and hence $p \mid \delta$, which is impossible. For $3p \nmid r$, we take (16) with

$$\alpha\beta^2 + p^2\gamma\delta^2 \equiv 0, \bmod r, \tag{17}$$

to form the combinations $\delta(17) - \gamma(16)$ and $\alpha(16) - \beta(17)$ that yield

$$\begin{aligned} \beta^2(\alpha\delta - \beta\gamma) = \pm\beta^2 \equiv 0, \bmod r^2; &\qquad \beta \equiv 0, \bmod r, \\ \text{and} \quad p^2\delta^2(\alpha\delta - \beta\gamma) = \pm p^2\delta^2 \equiv 0, \bmod r^2; &\qquad \delta \equiv 0, \bmod r, \end{aligned}$$

which cannot both hold for $|r| > 1$. Therefore $x^3 + p^2y^3$ belongs to a genus with one class only.

5. The final conclusions

Our theorems can now be stated

THEOREM 1. *Suppose the cubic polynomial $F(x)$ satisfies* Hypothesis P. *Suppose also that $f(u,v)$ is a fundamental cubic form and that the companion* $\mathrm{F}(x,y) = y^3F(x/y)$ *of $F(x)$ is contained in a fundamental form. Then identically*

$$F(x) = f(Ax+B, Cx+D)$$

for rational integers A, B, C, D.

Since we have shewn that Hypothesis P implies that the cubic fields corresponding to $f(u,v)$ and $\mathrm{F}(x,y)$ are the same, the two fundamental forms cited in the statement of the theorem are equivalent. Also $\mathrm{F}(x,y)$ contains the second fundamental form $f_2(u,v)$, say, and therefore contains the first by our compounding the substitution taking f_2 into F with the unimodular one taking f into f_2. Hence $\mathrm{F}(x,y) = f(Ax+By, Cx+Dy)$ and

$$F(x) = f(Ax+B, Cx+D).$$

There is also

THEOREM 2. *Suppose $F(x)$ satisfies* Hypothesis P. *Suppose also that $F(x)$ is primitive, $f(u,v)$ belongs to a (primitive) genus containing only one class, and that the greatest square factors of the discriminants of $F(x)$ and $f(u,v)$ are equal. Then*

$$F(x) = f(Ax+B, Cx+D)$$

for rational integers A, B, C, D satisfying $AD-BC = \pm 1$.

¿From the primitivity of $F(x)$ the identity (7) takes the form

$$k\mathrm{F}(x,y) = f(A_1x+B_1y, C_1x+D_1y).$$

Then, if $\triangle = A_1D_1 - B_1C_1$ and D_1, D_2 be the discriminants of $F(x)$ and $f(x,y)$,

$$k^4D_1 = |\triangle|^6D_2$$

and therefore $k^4 = |\triangle|^6$ by the hypothesis on D_1, D_2. For some non-zero integer r we thus have $k = r^3$, $\triangle = \pm r^2$, whence

$$\mathrm{F}(x,y) = f\left(\frac{A_1x}{r} + \frac{B_1y}{r}, \frac{C_1x}{r} + \frac{D_1y}{r}\right)$$

in which $\alpha = A_1/r$, $\beta = B_1/r$, $\gamma = C_1/r$, $\delta = D_1/r$ satisfy

$$\alpha\delta - \beta\gamma = \triangle/r^2 = \pm 1.$$

Consequently, being members of the same genus, $\mathrm{F}(x,y)$ and $f(u,v)$ are equivalent and the result follows.

References

[1] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, Vol 10, America Math. Soc., Providence, Rhode Island (1964).

[2] C. Hooley, On polynomials that are the sum of two cubes (to appear).

[3] F. Levi, Kubische Zahlkörper und binäre kubische Formenklassen, *Ber. Sachs. Akad. Wiss. Leipzig Mat.-Nat. Kl.* 66 (1914).

[4] A. Schinzel, On the relation between two conjectures on polynomials, Acta Arith., 36 (1980), 285-322.

Address

Cardiff School of Mathematics,
Cardiff University,
Senghennydd Road,
Cardiff,
CF24 4AG.

Received on 07-06-2006, Accepted on 13-06-2006