On Polynomials That Are Sums of Two Cubes

Christopher HOOLEY

Cardiff School of Mathematics
Cardiff University
Senghennydd Road
Cardiff, CF24 4AG — United Kingdom
reynishv@Cardiff.ac.uk

Received: May 24, 2006
Accepted: October 4, 2006

ABSTRACT

It is proved that, if $F(x)$ be a cubic polynomial with integral coefficients having the property that $F(n)$ is equal to a sum of two positive integral cubes for all sufficiently large integers n, then $F(x)$ is identically the sum of two cubes of linear polynomials with integer coefficients that are positive for sufficiently large x. A similar result is proved in the case where $F(n)$ is merely assumed to be a sum of two integral cubes of either sign. It is deduced that analogous propositions are true for cubic polynomials $F(x_0, \ldots, x_r)$ in more than one indeterminate.

Key words: polynomials, cubes.

2000 Mathematics Subject Classification: 11D32, 11P99.

Introduction

An area in the theory of numbers on which there has been intermittent speculation is typified by the question of whether, if $F(x_0, \ldots, x_r)$ be a polynomial with integer coefficients that assumes numerical values of a certain shape for all integer values of $x_0, \ldots, x_r$, then is $F(x_0, \ldots, x_r)$ identically of that shape. Subject to appropriate qualifications about the nature of the numbers N to be represented including their not forming sequences of positive density, the general response to such a question has been in the affirmative, although as yet there are not many instances where such a reaction has been substantiated. Among these are the cases where N is a perfect

ISSN: 1139-1138
http://dx.doi.org/10.5209/rev_REMA.2007.v20.n1.16569

power and where it is a sum of two squares that were settled, respectively, in 1913 and 1965 by Grosh (see [10]) and Davenport, Lewis, and Schinzel [2]. Following these was the case $N = u^k v^l$ $(k, l \geq 1)$ treated unconditionally by Schinzel [12], who continued by shewing that several important examples of the projected phenomenon can be established on the substantial assumption that appropriate sets of polynomials can simultaneously represent prime numbers.

As a contribution to this aspect of the theory of numbers, we consider here cubic polynomials with integral coefficients that are equal to sums of two cubes. In the first, and perhaps the most significant, part of the paper we shew that a cubic polynomial $F(x)$ in one variable with integral coefficients that equals a sum of two positive perfect cubes for integers $x > X_0$ is identically equal to the sum of two cubes of linear polynomials with integral coefficients (that are positive for $x > X_0'$). Then, having extended the analysis to the case where the cubes are not necessarily positive, we go on to consider cubics $F(x_0, \dots, x_r)$ that are sums of two cubes for all integers $x_0, \dots, x_r$ and deduce from our previous work that such cubics are also identically equal to the sum of two cubes of linear polynomials. In contrast to the earlier treatment the methods in the final part are more algebraical than analytical in nature and involve, in particular, a form of Grosh's result that we deem best proved here by an independent procedure. Potentially, however, there are other methods available for the case $r \geq 1$ but these would involve concepts we would wish to avoid on the present occasion.

It would be desirable to remove the restriction that $F(x)$ be cubic. But this would be to elevate the problem to a level of difficulty that we are presently unable to overcome, although there is little trouble involved in eliminating the possibility that $F(x)$ be linear or quadratic. We have not, however, exhausted the potentialities of these and other methods to the study of situations of this type and we therefore intend to return to them on future occasions.

1. Notation

Although the meaning of the notation should usually be clear from the context in which it arises, the following guide may be helpful. The letters x, x_0, $\dots$, x_r, ξ, t_1, $\dots$, t_r, denote variables or indeterminates in polynomials, where $(t_1, \dots, t_r)$ is written as $\mathbf{t}$; a, b, A, B, C, s are integers, save where the last is a complex variable; d, j, h, k, l, m, n, ν are integers that are usually positive; p is a positive prime number; for any integer denoted by δ, say, $\bar{\delta}$ is a solution of a congruence $\delta\bar{\delta} \equiv 1$, mod k, to a modulus k whose definition is evident from the context.

The letters X, Y are positive variables to be regarded as tending to infinity, all stated inequalities being true for sufficiently large values of X, Y; c, c_1,... are positive constants depending at most on the polynomials $F(x)$, $F(x_0, \dots, x_r)$ under consideration, as are the constants implied by the O-notation. The function $\sigma_{-\alpha}(m)$ is the sum $\sum_{d\,|\,m} d^{-\alpha}$.

2. Preparations

Our first study regarding polynomials $F(x)$ that are sums of two positive cubes requires some preparations that are also partially pertinent to our later investigations. The material involved is mostly embodied in a series of initial lemmata, to which others will be appended when the need for them arises.

By the substitution

$$r = \xi + \eta, \qquad s = \eta \tag{1}$$

of unit modulus the representability of a number as $\xi^3 + \eta^3$ with positive ξ, η is seen to be equivalent to that of the number by the form

$$f(r, s) = r(r^2 - 3rs + 3s^2),$$

wherein it may be assumed that $0 < s \leq \frac{1}{2}r$ by an interchange of ξ and η if necessary. Moreover, since the form $\xi^2 - \xi\eta + \eta^2$ to which $r^2 - 3rs + 3s^2$ is equivalent does not primitively admit prime divisors p that are congruent to 2, mod 3 even when $p = 2$, the divisibility of $f(r, s)$ by any such prime p implies that p divides r regardless of the sign of s. Availing ourselves of this property by introducing square-free numbers P (including 1) that are products (possibly empty) of such primes only, we shall need the following

Lemma 2.1. *Let $\tau(Y; h, k)$ be the number of integers P not exceeding Y that are congruent to h,* mod k. *Then, for given integers h, k such that either $(h, k) = 1$ or $(h, k) = 2$, we have*

$$\tau(Y; h, k) > \frac{cY}{\sqrt{\log Y}} \qquad (c = c(k) > 0)$$

for $Y > Y_0(h, k)$.

A sketch of the proof suffices, since it depends on standard contour integral methods and well-known properties of Dirichlet's L-functions. Yet, to ease the exposition in the latter case where $(h, k) = 2$, we limit our attention in the former case to the analogue $\tau'(Y; h, k)$ of $\tau(Y; h, k)$ that merely counts the odd numbers P' of type P appearing in the summation. Then, letting $\chi(n)$ denote a character, mod k, where $\chi_0(n)$ is principal, we set

$$\tau(Y, \chi) = \sum_{P' \leq Y} \chi(P')$$

and deduce in the usual way that

$$\tau'(Y; h, k) = \frac{1}{\phi(k)} \sum_{\chi} \overline{\chi}(h)\tau'(Y, \chi) \tag{2}$$

when $(h,k)=1$. The generating function of $\tau'(Y,\chi)$ being

$$T(s,\chi)=\sum_{P'}\frac{\chi(P')}{P'^s}=\prod_{\substack{p\equiv 2,\ \mathrm{mod}\ 3\\ p\neq 2}}\Big(1+\frac{\chi(p)}{p^s}\Big)$$

for $\sigma>1$, we form the characters

$$\chi^*(n)=\begin{cases}\big(\frac{-3}{n}\big)\chi(n), & \text{if } n \text{ be odd},\\ 0, & \text{if } n \text{ be even},\end{cases}$$

of modulus $[6,k]$ that appear in the Dirichlet's series

$$L(s,\chi^*)=\sum_{n=1}^{\infty}\frac{\chi^*(n)}{n^s}=\prod_{p\neq 2}\Big(1-\frac{\chi^*(p)}{p^s}\Big)^{-1}.$$

Then

$$\begin{aligned}\frac{L(s,\chi)}{L(s,\chi^*)}&=\Big(1-\frac{\chi(2)}{2^s}\Big)^{-1}\prod_{\substack{p\equiv 2,\ \mathrm{mod}\ 3\\ p\neq 2}}\Big(1-\frac{\chi(p)}{p^s}\Big)^{-1}\Big(1+\frac{\chi(p)}{p^s}\Big)\\ &=\Big(1-\frac{\chi(2)}{2^s}\Big)^{-1}\prod_{\substack{p\equiv 2,\ \mathrm{mod}\ 3\\ p\neq 2}}\Big(1-\frac{\chi^2(p)}{p^{2s}}\Big)^{-1}\prod_{\substack{p\equiv 2,\ \mathrm{mod}\ 3\\ p\neq 2}}\Big(1+\frac{\chi(p)}{p^s}\Big)^{2}\\ &=\Big(1-\frac{\chi(2)}{2^s}\Big)^{-1}\prod_{\substack{p\equiv 2,\ \mathrm{mod}\ 3\\ p\neq 2}}\Big(1-\frac{\chi^2(p)}{p^{2s}}\Big)^{-1}T^2(s,\chi)\\ &=Z(s,\chi)T^2(s,\chi),\end{aligned}$$

say, where $Z(s,\chi)$ defines a function that is regular and non-zero for $\sigma>\frac{1}{2}$. Hence

$$T(s,\chi)=\sqrt{\frac{L(s,\chi)}{L(s,\chi^*)}}\sqrt{Z(s,\chi)},$$

in the right-hand side of which at $s=1$ the function $L(s,\chi)$ only has a pole when $\chi=\chi_0$ and $L(s,\chi^*)$ never has a zero (indeed, it may have a pole when $\chi\neq\chi_0$ and χ^* is principal). Therefore, by the arguments used for example by Wilson [16], we infer that

$$\tau'(Y,\chi_0)>\frac{2c_1(k)Y}{\sqrt{\log Y}}$$

and

$$\tau'(Y,\chi)=O\Big(\frac{Y}{\log Y}\Big)\qquad(\chi\neq\chi_0),$$

from which and (2) the required result flows for the case $(h,k)=1$; the result in the second case $(h,k)=2$ is then an obvious corollary because the numbers P to be counted are of the type $2P'$.

In much the same vein there is also

Lemma 2.2. *Let $\tau_1(Y;h,k)$ be defined like $\tau(Y;h,k)$ in the statement of Lemma 2.1 save that the numbers P it counts are to have prime factors that all exceed some given positive constant c. Then, for $(h,k)=1$, we have*

$$\tau_1(Y;h,k)\to\infty$$

as $Y\to\infty$.

The demonstrations will also bear upon some properties — of various degrees of familiarity — of irreducible polynomials $f(x)$ with integer coefficients, of which the polynomials $F(x)$ under investigation are the usual but not exclusive examples. First we need a result related to the elementary theory of congruences and then estimates that flow from the prime ideal theorem and a classical principle due to Dedekind — for the former see Nagell [9, chapter 3] and for the latter see Erdös [3].

Lemma 2.3. *Let $f(x)$ be an irreducible polynomial with integer coefficients and let $\rho^*(k)$ be the number of incongruent solutions of $f(\nu)\equiv 0, \bmod k$. Then*

(i)
$$\rho^*(k_1k_2)=O\{\rho^*(k_1)\rho^*(k_2)\},$$

(ii)
$$\sum_{k\le y}\rho^*(k)=O(y),$$

(iii)
$$\prod_{p\le y}\left(1+\frac{\rho^*(p)}{p}\right)\sim c(f)\log y \qquad (c(f)>0),$$

where the constants implied by the O-notation depend at most on the coefficients of $f(x)$.

We shall also depend on the following variant of our findings in our paper [6] regarding the uniform distribution of the roots of polynomial congruences. In this, we should note that a part is played by the previous lemma, which, however, has been stated here because of its significance in our later analysis.

Lemma 2.4. *For any irreducible cubic polynomial $f(x)$ let*

$$S(h_1,k)=\sum_{\substack{f(\nu)\equiv 0,\ \mathrm{mod}\ k\\ 0<\nu\le k}} e^{2\pi i h_1\nu/k}.$$

Then, for any positive integers d and h, we have

$$R(h,X_1)=\sum_{\substack{k\le X_1\\ (k,\bar{d})=1}}|S(h\bar{d}^{\,2},k)|=O\Big(\frac{\sigma_{-\frac14}(h)X_1}{\log^{\frac16}X_1}\Big), \tag{3}$$

where the constants implied by the O-notation depend at most on the coefficients of $f(x)$.

To explain the lemma we temporarily adopt the notation and conventions of our paper [6], bearing in mind that they are at variance with those adopted in other places here. Apart from the unimportant possibility that $f(x)$ may be imprimitive, which is easily handled through the use of its discriminant D, the main differences between (3) and the estimate in Theorem 1 of [6] are the presence of $\bar{d}$ in the exponential and the identification of $\sigma_{-\frac14}(h)$ as a legitimate choice for $C_9(h)$, since in the earlier paper it is clear that the summand $S(h,k)$ in $R(x,k)$ may be replaced by its modulus. To react to the new situation we first restrict all numbers of the type k_1, k_2, l_2, etc., previously occurring to be relatively prime to d, whereupon we see that equations (1) to (8) in [6] are still valid under the new interpretation. Next the analogue of the equation following (8) becoming

$$\begin{aligned}\sum\nolimits_6 &= \sum_{\substack{0<a\le k_1\\ (a,k_1)=1}}|S(a\bar{d}^{\,2}h,k_1)|\sum_{\substack{k_2\le y\\ k_2\equiv\bar{a},\ \mathrm{mod}\ k_1}}1\\ &= \sum_{\substack{0<a\le k_1\\ (a,k_1)=1}}|S(ah,k)|\sum_{\substack{k_2\le y\\ k_2\equiv\bar{a}\bar{d}^{\,2},\ \mathrm{mod}\ k_1}}1\end{aligned}$$

because $(d,k_1)=(d,k_2)=1$ and $d\bar{d}\equiv 1,\ \mathrm{mod}\ k_1$, we deduce that the new $\sum_6$ adheres to (9) and hence that the new $\sum_1$ satisfies

$$\sum\nolimits_1 = O\Big(\frac{x(\log\log x)^5}{\log x}\sum_{l\le x}\frac{(l,h)^{\frac12}\rho^{\frac12}(l)}{l^{\frac12}\phi^{\frac12}(l)}\Big).$$

The sum in this is not greater than

$$\begin{aligned}\sum_{d\,|\,h}d^{\frac12}\sum_{l'\le x/d}\frac{\rho^{\frac12}(dl')}{(dl')^{\frac12}\phi^{\frac12}(dl')} &= O\Big(\sum_{d\,|\,h}\frac{\rho^{\frac12}(d)}{\phi^{\frac12}(d)}\sum_{l\le x}\frac{\rho^{\frac12}(l)}{l^{\frac12}\phi^{\frac12}(l)}\Big)\\ &= O\Big(\frac{\log x}{\log^{\delta_3}x}\sum_{d\,|\,h}\frac{\rho^{\frac12}(d)}{\phi^{\frac12}(d)}\Big)\end{aligned}$$

by Lemma 2.3 (i) and by the estimate for (the original) $\sum_7$ supplied in [6]. As for the divisor sum, it is

$$O\Big(\sum_{d\,|\,h}\frac{(2\sqrt{3})^{\omega(d)}}{d^{\frac12}}\Big)=O\Big[\prod_{p\,|\,h}\Big\{1+\frac{4}{p^{\frac12}}\Big(1-\frac{1}{p^{\frac12}}\Big)^{-1}\Big\}\Big]$$
$$=O\Big\{\prod_{p\,|\,h}\Big(1+\frac{16}{p^{\frac12}}\Big)\Big\}=O\{\sigma_{-\frac14}(h)\},$$

and the lemma follows by the final reasoning that preceded the deduction of Theorem 1 in [6] and by then replacing x by X_1.

Our final lemma in this section is on trigonometrical approximations to the function

$$\psi(t)=[t]+\frac12-t \tag{4}$$

and is the main instrument in the application of Lemma 2.4 to our problem. This is expressed in the accurate form due to Vaaler [14], although earlier less exact forms would suffice for our present purpose.

Lemma 2.5. *For any positive integer N there are coefficients $\mathrm{c}_{h,N}=\mathrm{c}_h=O(1/|h|)$ and $\mathrm{c}'_h=O(1/N)$ for $0<|h|\le N$ and $0\le|h|\le N$, respectively, with the property that*

$$\psi(t)=\sum_{0<|h|\le N}\mathrm{c}_h e^{2\pi iht}+O\Big(\sum_{|h|\le N}\mathrm{c}'_h e^{2\pi iht}\Big),$$

the series within the O-symbol being real and non-negative.

3. Adoption of the Hypothesis P; the reducibility of $F(x)$

We are ready to examine the implications of

Hypothesis P. *$F(x)$ is a cubic polynomial with integral coefficients having the property that $F(n)$ is equal to a sum of two positive integral cubes for all sufficiently large integers n and thus for all n exceeding some integer n_0.*

We demonstrate that $F(x)$ is not irreducible by assuming the opposite and counting the number $\Upsilon(X)$ of solutions of the equation

$$r(r^2-3rs+3s^2)=F(n) \tag{5}$$

in integers r, s, and n for which

$$n_0<n\le X,\qquad 0<s\le\frac12 r. \tag{6}$$

Since

$$r^2 - 3rs + 3s^2 = \frac{1}{4}r^2 + 3\Big(s - \frac{1}{2}r\Big)^2 \tag{7}$$

and therefore

$$\frac{1}{4}r^2 \le r^2 - 3rs + 3s^2 < r^2, \tag{8}$$

the conditions governing the definition of $\Upsilon(X)$ imply that

$$\frac{1}{4}r^3 < c_1X^3 \qquad \text{and} \qquad c_2n^3 < r^3$$

so that

$$r \le c_3X \qquad \text{and} \qquad n \le c_4r. \tag{9}$$

Also, on writing (5) in the form

$$rm = F(n)$$

and noting that no value of m can be presented more that once when r and n are given, we now form a workable envelope for the numbers m occurring by using the already stated impossibility of the simultaneous relations

$$p \,|\, m, \qquad p^2 \nmid m \tag{10}$$

when p is a prime congruent to 2, mod 3. To this end, we take a number $\zeta = \zeta(X)$ to be chosen explicitly later and cover the set of eligible numbers for each r by those m that do not have the property (10) for each prime p conforming to the basic conditions

$$p \equiv 2, \bmod 3, \qquad c_5 < p \le \zeta, \tag{11}$$

and the supplementary condition

$$p \nmid r \tag{12}$$

for a sufficiently large value of c_5. Then, in preparation for the usual exclusion process associated with Legendre, we introduce square-free products d (including 1) of primes p of type (11), which are governed by the bound

$$d \le \prod_{\substack{p\le\zeta \\ p\equiv 2,\ \mathrm{mod}\ 3}} p < \exp\Big(\sum_{p\le\zeta} \log p\Big) < e^{c_6\zeta} = Z, \tag{13}$$

say, and use the symbolism $d \,\|\!|\, m$ to indicate that $p \,\|\, m$ for each prime factor p of d. (We do not use the notation $d \,\|\, m$, because this might be interpreted as meaning that d was the highest power of d dividing m). Accordingly, by (9), we find that

$$\Upsilon(X) \le \sum_{r\le c_3X} \sum_{\substack{rm=F(n) \\ n\le c_4r}} \sum_{\substack{d \,\|\!|\, m \\ (d,r)=1}} \mu(d) = \sum_{r\le c_3X} \Upsilon_r(X), \tag{14}$$

say, and complete the first phase of the estimation.

To proceed from this inequality we note that for a given number d the condition $d \| m$ is tantamount to the simultaneous conditions $d \mid m$, $(m/d, d) = 1$ that mean that

$$m \equiv ld, \bmod d^2, \tag{15}$$

for some number l satisfying

$$0 < l \le d, \qquad (l, d) = 1. \tag{16}$$

Therefore, changing the order of summations in $\Upsilon_r(X)$, we have

$$\begin{aligned} \Upsilon_r(X) &= \sum_{(d,r)=1} \mu(d) \sum_{\substack{0<l\le d \\ (l,d)=1}} \sum_{\substack{n\le c_4 r \\ F(n)\equiv rld, \bmod rd^2}} 1 \\ &= \sum_{(d,r)=1} \mu(d) \Upsilon_{d,r}, \end{aligned} \tag{17}$$

say, where the primary condition

$$F(n) \equiv rld, \bmod rd^2, \tag{18}$$

within the innermost sum is the conjunction of the conditions

$$F(n) \equiv 0, \bmod r, \tag{19}$$

and

$$F(n) \equiv rld, \bmod d^2, \tag{20}$$

because $(d, r) = 1$ by (12). Next this innermost sum equals

$$\begin{aligned} \sum_{\substack{0<\Omega\le rd^2 \\ F(\Omega)\equiv rld, \bmod rd^2}} \sum_{\substack{n\le c_4 r \\ n\equiv\Omega, \bmod rd^2}} 1 \;&=\; \sum_{\substack{0<\Omega\le rd^2 \\ F(\Omega)\equiv rld, \bmod rd^2}} \left(\left[\frac{c_4 r - \Omega}{rd^2} \right] - \left[\frac{-\Omega}{rd^2} \right] \right) \\ &= \frac{c_4}{d^2} \sum_{\substack{0<\Omega\le rd^2 \\ F(\Omega)\equiv rld, \bmod rd^2}} 1 \\ &\quad + \sum_{\substack{0<\Omega\le rd^2 \\ F(\Omega)\equiv rld, \bmod rd^2}} \left\{ \psi\left(\frac{c_4 r - \Omega}{rd^2} \right) - \psi\left(\frac{-\Omega}{rd^2} \right) \right\} \end{aligned}$$

in the notation of (4), whence

$$\begin{aligned}\Upsilon_{d,r} &= \frac{c_4}{d^2}\sum_{\substack{0<l\le d\\(l,d)=1}}\sum_{\substack{0<\Omega\le rd^2\\F(\Omega)\equiv rld,\ \mathrm{mod}\ rd^2}}1\\ &\quad+\sum_{\substack{0<l\le d\\(l,d)=1}}\sum_{\substack{0<\Omega\le rd^2\\F(\Omega)\equiv rld,\ \mathrm{mod}\ rd^2}}\left\{\psi\left(\frac{c_4 r-\Omega}{rd^2}\right)-\psi\left(\frac{-\Omega}{rd^2}\right)\right\}\\ &= \frac{c_4}{d^2}\Upsilon^*_{d,r}+\Upsilon^\dagger_{d,r},\end{aligned}\tag{21}$$

say. Thus, letting $\Upsilon^*(X)$ and $\Upsilon^\dagger(X)$ be the respective contributions to $\Upsilon(X)$ due to $(c_4/d^2)\Upsilon^*_{d,r}$ and $\Upsilon^\dagger_{d,r}$ via (17) and (14) so that

$$\Upsilon(X)=\Upsilon^*(X)+\Upsilon^\dagger(X)\tag{22}$$

in particular, we get the equations

$$\Upsilon^*(X)=c_4\sum_{r\le c_3X}\sum_{(d,r)=1}\frac{\mu(d)}{d^2}\Upsilon^*_{d,r}\tag{23}$$

and

$$\Upsilon^\dagger(X)=\sum_d\mu(d)\sum_{\substack{r\le c_3X\\(r,d)=1}}\Upsilon^\dagger_{d,r}\tag{24}$$

that are to be separately developed.

Starting with $\Upsilon^*(X)$, we extend a notation associated with the verification of Lemma 2.4 by letting $\rho(r)$ be the number of incongruent roots, $\mathrm{mod}\, r$, of (19) and then continue by letting $\upsilon(r,l,d)$ be the number of incongruent roots of (20). Then, by the comment on (18),

$$\Upsilon^*_{d,r}=\rho(r)\sum_{\substack{0<l\le d\\(l,d)=1}}\upsilon(r,l,d)=\rho(r)\sum_{\substack{0<l\le d\\(l,d)=1}}\upsilon(1,l,d),$$

the last sum in which through (15) and (16) is equal to the number of incongruent n, $\mathrm{mod}\, d^2$, for which $d\,|||\, F(n)$. Hence, as the prime factors of d exceed c_5,

$$\sum_{0<l\le d}\upsilon(r,l,d)=\prod_{p\,|\,d}\{p\rho(p)-\rho(p^2)\}=\prod_{p\,|\,d}(p-1)\rho(p)=\phi(d)\rho(d),\tag{25}$$

and we infer from (23) that

$$\begin{aligned}\Upsilon^*(X) &= c_4 \sum_{r\le c_3X} \rho(r) \sum_{(d,r)=1} \frac{\mu(d)\phi(d)\rho(d)}{d^2} \\ &= c_4 \sum_{r\le c_3X} \rho(r) \prod_{\substack{c_5<p\le\zeta \\ p\nmid r; p\equiv 2,\ \mathrm{mod}\ 3}} \left(1-\frac{(p-1)\rho(p)}{p^2}\right) \\ &= c_4 \sum_{r\le c_3X} \rho(r)\psi_r(\zeta), \end{aligned} \tag{26}$$

say, in which

$$\begin{aligned}\psi_r(\zeta) &\le \psi_1(\zeta) \prod_{\substack{p\,|\,r \\ p>3}} \left(1-\frac{(p-1)\rho(p)}{p^2}\right)^{-1} \le \psi_1(\zeta) \prod_{\substack{p\,|\,r \\ p>3}} \left(1-\frac{3}{p}\right)^{-1} \\ &\le c_7\psi_1(\zeta) \prod_{p\,|\,r} \left(1+\frac{3}{p}\right) = c_7\psi_1(\zeta)\sigma^*(r), \end{aligned} \tag{27}$$

say. Also

$$\begin{aligned}\psi_1(\zeta) &\le \prod_{\substack{c_5<p\le\zeta \\ p\equiv 2,\ \mathrm{mod}\ 3}} \left(1+\frac{(p-1)\rho(p)}{p^2}\right)^{-1} = \prod_{\substack{c_5<p\le\zeta \\ p\equiv 2,\ \mathrm{mod}\ 3}} \left(1+\frac{\rho(p)}{p}\right)^{-1} \prod_{\substack{c_5<p\le\zeta \\ p\equiv 2,\ \mathrm{mod}\ 3}} \left\{1+O\left(\frac{1}{p^2}\right)\right\} \\ &\le c_8 \prod_{c_5<p\le\zeta} \left(1+\frac{\rho(p)}{p}\right)^{-1} \prod_{\substack{c_5<p\le\zeta \\ p\equiv 1,\ \mathrm{mod}\ 3}} \left(1+\frac{\rho(p)}{p}\right) \\ &\le c_9 \prod_{c_5<p\le\zeta} \left(1+\frac{\rho(p)}{p}\right)^{-1} \prod_{\substack{c_5<p\le\zeta \\ p\equiv 1,\ \mathrm{mod}\ 3}} \left(1+\frac{2\rho(p)}{p}\right)^{\frac{1}{2}} \\ &= \frac{c_9\Psi_2^{\frac{1}{2}}(\zeta)}{\Psi_1(\zeta)}, \end{aligned} \tag{28}$$

say. Here

$$\Psi_1(\zeta) > c_{10}\log\zeta \tag{29}$$

by Lemma 2.3, which also estimates the other product through the intercession of

Lemma 3.1. *Let $f_1(x)$ and $f_2(x)$ be given irreducible polynomials with integral coefficients and co-prime degrees ∂_1 and ∂_2, the number of incongruent roots of the congruence $f_i(x) \equiv 0, \mod p$, being denoted by $\rho_i(p)$ for $i = 1$ and 2. Then there*

is an irreducible polynomial $f_3(x)$ with integral coefficients and degree $\partial_1\partial_2$ with the property that the number $\rho_3(p)$ of incongruent roots of $f_3(x) \equiv 0, \bmod p$, is given by

$$\rho_3(p) = \rho_1(p)\rho_2(p)$$

for all $p > c_5$.

Although presumably well-known, this result does not seem to have been explicitly enunciated in the literature. It is, however, easily demonstrated by ideal theory; alternatively, there is a more elementary method on which it would be inappropriate to comment on the present occasion.

Take $f_1(x)$ and $f_2(x)$ in the lemma to be the given cubic polynomial (assumed irreducible) $F(x)$ and $x^2 + x + 1$ so that $\rho_3(p)$ becomes $2\rho(p)$ or 0 according as $p \equiv 1, \bmod 3$, or $p \equiv 2, \bmod 3$. Hence, having seen that

$$\Psi_2(\zeta) < c_{11} \log \zeta,$$

we deduce from (29) and (28) the inequality

$$\psi_1(\zeta) < \frac{c_{12}}{\sqrt{\log \zeta}},$$

which implies that

$$\Upsilon^*(X) < \frac{c_{13}}{\sqrt{\log \zeta}} \sum_{r \le c_3 X} \rho(r)\sigma^*(r)$$

in virtue of (26) and (27). Finally, since

$$\sigma^*(r) \le \sum_{j|r} \frac{3^{\omega(j)}\mu^2(j)}{j},$$

we have from Lemma 2.3 that

$$\begin{aligned}
\sum_{r \le c_3 X} \rho(r)\sigma^*(r) &\le \sum_{jr' \le c_3 X} \frac{3^{\omega(j)}\mu^2(j)\rho(jr')}{j} \\
&\le c_{14} \sum_{jr' \le c_3 X} \frac{3^{\omega(j)}\mu^2(j)\rho(j)\rho(r')}{j} \\
&\le c_{14} \sum_{j \le c_3 X} \frac{9^{\omega(j)}}{j} \sum_{r' \le c_3 X/j} \rho(r') \\
&\le c_{15} X \sum_{j \le c_3 X} \frac{9^{\omega(j)}}{j^2} \le c_{16} X
\end{aligned}$$

with the conclusion that

$$\Upsilon^*(X) = O\Big(\frac{X}{\sqrt{\log\zeta}}\Big). \tag{30}$$

To estimate $\Upsilon^\dagger(X)$ we return to the sum $\Upsilon^\dagger_{d,r}$ in (21) whose treatment entails the introduction of the exponential sums

$$\begin{aligned} U_1(h,r,l,d) &= \sum_{\substack{0<\Omega\le rd^2\\ F(\Omega)\equiv rld,\ \mathrm{mod}\ rd^2}} e^{2\pi i h\Omega/rd^2},\\ U(h,r,d) &= \sum_{\substack{0<l\le d\\ (l,d)=1}} U_1(h,r,l,d),\\ S(h_1,r) &= \sum_{\substack{0<\nu\le r\\ F(\nu)\equiv 0,\ \mathrm{mod}\ r}} e^{2\pi i h_1\nu/r},\\ u(h_2,r,l,d) &= \sum_{\substack{0<\nu_1\le d^2\\ F(\nu_1)\equiv rld,\ \mathrm{mod}\ d^2}} e^{2\pi i h_2\nu_1/d^2}, \end{aligned} \tag{31}$$

the last of which is bounded in magnitude by its specialization $\upsilon(r,l,d)$ taken when $h_2 = 0$. Since by a familiar process in the handling of exponential sums (see, for example, Lemma 3 in [8]) the assumed coprimality of r and d implies the multiplicative relation

$$U_1(h,r,l,d) = S(h\bar{d}^2, r)u(h\bar{r}, r, l, d),$$

we deduce first that

$$U(h,r,d) = S(h\bar{d}^2, r) \sum_{\substack{0<l\le d\\ (l,d)=1}} u(h\bar{r}, r, l, d),$$

and therefore that

$$\begin{aligned} |U(h,r,d)| &\le |S(h\bar{d}^2, r)| \sum_{\substack{0<l\le d\\ (l,d)=1}} \upsilon(r,l,d)\\ &= \rho(d)\phi(d)|S(h\bar{d}^2, r)| \end{aligned} \tag{32}$$

by (25). This inequality suffices for our purposes although a sharper one can be obtained by the replacement of $\phi(d)$ by a smaller entity.

By (21) and by Lemma 2.5 with a suitable value of $N = N(X)$ to be chosen soon,

we have

$$\begin{aligned}\Upsilon^{\dagger}_{d,r} &= \sum_{\substack{0<l\le d\\(l,d)=1}} \sum_{\substack{0<\Omega\le rd^2\\ F(\Omega)\equiv rld,\ \mathrm{mod}\ rd^2}} \Bigg\{ \sum_{0<|h|\le N} \mathrm{c}_h\big(e^{2\pi i h(c_4 r-\Omega)/rd^2} - e^{-2\pi i h\Omega/rd^2}\big) \\ &\quad + O\Bigg(\sum_{0\le|h|\le N} \mathrm{c}'_h\big(e^{2\pi i h(c_4 r-\Omega)/rd^2} + e^{-2\pi i h\Omega/rd^2}\big)\Bigg)\Bigg\} \\ &= \sum_{\substack{0<l\le d\\(l,d)=1}} \sum_{\substack{0<\Omega\le rd^2\\ F(\Omega)\equiv rld,\ \mathrm{mod}\ rd^2}} \sum_{0<|h|\le N} \mathrm{c}_h\big(e^{2\pi i h(c_4 r-\Omega)/rd^2} - e^{-2\pi i h\Omega/rd^2}\big) \\ &\quad + O\Bigg(\sum_{\substack{0<l\le d\\(l,d)=1}} \sum_{\substack{0<\Omega\le rd^2\\ F(\Omega)\equiv rld,\ \mathrm{mod}\ rd^2}} \sum_{0\le|h|\le N} \mathrm{c}'_h\big(e^{2\pi i h(c_4 r-\Omega)/rd^2} + e^{-2\pi i h\Omega/rd^2}\big)\Bigg),\end{aligned}$$

from which, changing the order of summations and using both (31) and then (32) with $r\neq 0$ and $h=0$, we deduce that

$$\begin{aligned}|\Upsilon^{\dagger}_{d,r}| &\le 2\sum_{0<|h|\le N} |\mathrm{c}_h||U(h,r,d)| + O\Bigg(\sum_{0\le|h|\le N} |\mathrm{c}'_h||U(h,r,d)|\Bigg) \\ &= O\Big(\frac{U(0,r,d)}{N}\Big) + O\Bigg(\sum_{0<h\le N}\frac{|U(h,r,d)|}{h}\Bigg) \\ &= O\Big(\frac{\rho(d)\phi(d)\rho(r)}{N}\Big) + O\Bigg(\rho(d)\phi(d)\sum_{0<h\le N}\frac{|S(h\bar{d}^2,r)|}{h}\Bigg).\end{aligned}$$

The first term on the last line of the above inequality provides by way of (24) and (13) a donation of

$$O\Big(\frac{Z}{N}\sum_{r\le c_3X}\rho(r)\sum_{d\le Z}\rho(d)\Big) = O\Big(\frac{Z^2X}{N}\Big)$$

to $\Upsilon^{\dagger}(X)$, whereas the effect of the second term is

$$\begin{aligned}O\Bigg(Z\sum_{d\le Z}\rho(d)\sum_{0<h\le N}\frac{1}{h}\sum_{\substack{r\le c_3X\\(r,d)=1}}|S(h\bar{d}^2,r)|\Bigg) &= O\Bigg(\frac{ZX}{\log^{\frac16}X}\sum_{d\le Z}\rho(d)\sum_{0<h\le N}\frac{\sigma_{-\frac14}(h)}{h}\Bigg) \\ &= O\Big(\frac{Z^2X\log N}{\log^{\frac16}X}\Big)\end{aligned}$$

by Lemmata 2.3 and 2.4. Let us therefore now set $N = [\log^{\frac{1}{6}} X]$, whereupon we get the estimate

$$\Upsilon^{\dagger}(X) = O\Big(\frac{Z^2 X}{\log^{\frac{1}{7}} X}\Big).$$

The estimate we seek flows from this, (22), and (30), which imply that

$$\begin{aligned}\Upsilon(X) &= O\Big(\frac{X}{\sqrt{\log \zeta}}\Big) + O\Big(\frac{Z^2 X}{\log^{\frac{1}{7}} X}\Big) \\ &= O\Big(\frac{X}{\sqrt{\log\log\log X}}\Big) \end{aligned} \tag{33}$$

if in (11) and (13) we take

$$\zeta = \frac{1}{15c_6}\log\log x$$

and therefore

$$Z = \log^{\frac{1}{15}} X.$$

But this is inconsistent with the inequality

$$\Upsilon(X) \geq X - n_0$$

that stems from Hypothesis P, and we therefore deduce that $F(x)$ is reducible.

4. The proof of the first theorem completed

Having shewn that $F(x)$ must be reducible, we first dispose of the special case in which $F(x)$ is of the form

$$D(ax+b)^3, \tag{34}$$

where $a > 0$ (by the form of Hypothesis P) and where it may be assumed that $(a,b) = 1$. To do this we shun any reference to the theory of elliptic curves but instead take the constant c in the statement of Lemma 2.2 to satisfy

$$c > \sqrt[3]{4D} = c_{17},$$

say, and choose in accordance with this lemma some integer n exceeding n_0 for which $an+b$ is a square-free number P whose prime factors exceed c. Then the equation

$$DP^3 = D(an+b)^3 = f(r,s) = rg(r,s)$$

being soluble in positive integers r, s, we have $P \,|\, r$ by our preparatory remarks and thus $r = Pl$ for some positive integer l. However, since

$$f(r,s) \geq \frac{1}{4}r^3$$

by (7), it follows that

$$\frac{1}{4}l^3P^3 \leq DP^3$$

so that $l < c$. Hence, from

$$DP^2 = l(l^2P^2 - 3lPs + 3s^2), \tag{35}$$

we deduce that $P \,|\, s$ and $s = l_1P$ with $0 < l_1 \leq \frac{1}{2}l$, wherefore

$$D = l(l^2 - 3ll_1 + 3l_1^2) = (l - l_1)^3 + l_1^3.$$

Therefore in this case

$$F(x) = \{(l - l_1)(ax + b)\}^3 + \{l_1(ax + b)\}^3, \tag{36}$$

as desired.

In all other cases, being cubic, $F(x)$ has at least one integral linear factor and may therefore be expressed in the not yet necessarily unique form

$$(ax + b)(Ax^2 + Bx + C),$$

where $(a, b) = 1$ and a, A are positive. Associated with the polynomial as thus written, there are the determinant

$$\triangle = B^2 - 4AC \tag{37}$$

of the second factor and the resultant

$$R = Ab^2 - Bab + Ca^2, \tag{38}$$

not both of which can vanish in the situation we are now in. Then, to execute the demonstration further, we shall need the services of a suitable sequence $\mathcal{S}$ of positive integers n for which $an+b$ is of the form P, the number $t(X)$ of such n up to X being subject to an inequality of the type

$$t(X) > \frac{cX}{\sqrt{\log X}} \tag{39}$$

for some small positive constant $c = c(F)$. Initially left unspecified, this sequence will be later defined through Lemma 2.1 in the light of subsequent experience in such a way that its earlier use is justified. (In fact its choice will only depend on the coefficients a, b, c, A, and B.)

As the equation

$$(an + b)(An^2 + Bn + C) = r(r^2 - 3rs + 3s^2) \tag{40}$$

is always soluble for $n > n_0$, we deduce that for any large n in $\mathcal{S}$ we have $(an + b) \,|\, r$ and thus

$$r = l(an + b) \tag{41}$$

for some positive integer l, the next implication being that

$$An^2 + Bn + C = l(r^2 - 3rs + 3s^2) \tag{42}$$

where again for convenience we still assume that

$$s \leq \frac{1}{2}r \tag{43}$$

in virtue of an early remark in section 2. On the other hand, by (40) and (8), we have the inequality

$$D_1(an+b)^3 > \frac{1}{4}r^3$$

for some suitable positive number D_1 and thus

$$r < \sqrt[3]{4D_1}(an+b),$$

which inequality shews that

$$0 < l < \sqrt[3]{4D_1} = c_{18} \tag{44}$$

in (41).

For each of the finite number of possible values l_1 of l in (44) let us consider the number of integers n in $\mathcal{S}$ that answer to it by way of (41) and (42), where it must be borne in mind that the same n might correspond to more than one l_1 because the number of ways of representing a number as the sum of two cubes is not always essentially unique. We have

$$An^2 + Bn + C = l_1\{l_1^2(an+b)^2 - 3l_1(an+b)s + 3s^2\}$$

and therefore

$$4(An^2 + Bn + C) - l_1^3(an+b)^2 = 3l_1\{2s - l_1(an+b)\}^2,$$

which equality we write as

$$A_1n^2 + B_1n + C_1 = 3l_1\{2s - l_1(an+b)\}^2 \tag{45}$$

where $A_1 = A_1(l_1)$, $B_1 = B_1(l_1)$, $C_1 = C_1(l_1)$ cannot all be zero. If the determinant $\square(l_1)$ of the quadratic $A_1x^2 + B_1x + C_1$ be non-zero, then the equation takes the form of either

$$B_1n + C_1 = 3l_1\{2s - l_1(an+b)\}^2 \qquad (A_1 = 0, \quad B_1 \neq 0)$$

or

$$(2A_1n + B_1)^2 - 12A_1l_1\{2s - l_1(an+b)\}^2 = \square(l_1) \qquad (A_1 \neq 0).$$

In the first of these $B_1n + C_1$ is a fixed multiple of a perfect square and there are consequently only $O(X^{\frac{1}{2}})$ possible values of n whereas in the second the number of n

is $O(\log X)$ by a customary argument involving the Pellian equation and the theory of indefinite quadratic forms. (For an example of this reasoning, see [5].) Hence the majority of values of n in $\mathcal{S}$ that relate to (45) correspond to a zero l of $\square(l)$, having indeed a cardinality exceeding

$$\frac{cX}{\sqrt{\log X}} - c_{19}X^{\frac{1}{2}} > \frac{cX}{2\sqrt{\log X}}.$$

Moreover, since

$$\begin{aligned}\square(l) &= (4B - 2abl^3)^2 - 4(4A - l^3a)(4C - l^3b)\\ &= 16(\triangle - Rl^3)\end{aligned}$$

by (45), (37), and (38), the vanishing of $\square(l)$ is equivalent to

$$\triangle = Rl^3, \tag{46}$$

which has a unique solution because $\triangle$ and R are not both zero. (Indeed, it is now seen that neither $\triangle$ nor R is non-zero.) In the major case thus isolated when (46) holds, we may therefore write

$$A_1x^2 + B_1x + C_1 = m(A_2x + B_2)^2,$$

where $(A_2, B_2) = 1$, $A_2 \geq 0$, and m is a positive integer, and the equality (45) becomes

$$m(A_2n + B_2)^2 = 3l\{2s - l(an + b)\}^2. \tag{47}$$

In the simplest instance where $A_2 = 0$, we have $B_2 = 1$ with the deduction that $3l \,|\, m$, $m = 3l\mu^2$ with $\mu > 0$, and

$$\mu^2(A_2n + B_2)^2 = \{2s - l(an + b)\}^2. \tag{48}$$

In this case the choice of the sequence $\mathcal{S}$ is particularly easy because no restriction on the numbers P to be represented by $an + b$ is needed, wherefore we derive (39) by using Lemma 2.1 with $h = b$, $k = a$, and $Y = aX + b$. But in the other cases to be considered the choice of $\mathcal{S}$ is more complicated because it must depend in part on the integer l defined by (46).

When $A_2 \neq 0$ we let l_2 denote the square-free product of the prime divisors of $3l$. Suppose first that l be odd. Then, for any prime divisor p of l_2, the congruential conditions

$$A_2H_p + B_2 \not\equiv 0, \bmod p, \qquad aH_p + b \not\equiv 0, \bmod p, \tag{49}$$

have at least one solution H_p, $\bmod p$, because there are at most two incongruent values of H_p for which either $A_2H_p + B_2 \equiv 0, \bmod p$ or $aH_p + b \equiv 0, \bmod p$. There being therefore a residue class $H, \bmod l_2$, for which

$$(A_2H + B_2, l_2) = (aH + b, l_2) = 1, \tag{50}$$

we consider the numbers $an+b$ in which n is limited to be of the form $n_1 = H + ql_2$. Since these constitute an arithmetical progression $aH+b+aql_2$ where $(aH+b, al_2) \leq (b,a)(aH+b, l_2) = 1$, we form a sequence of n_1 of type $\mathcal{S}$ by requiring that $an_1 + b$ be a number P and by using Lemma 2.1 with $h = aH + b$, $k = al_2$, and $Y = aX + b$. Therefore, on taking any value of $n = n_1$, for which (47) applies, we deduce that $3l \,|\, m$ and thus recoup (48).

A slight adjustment in the above procedure is called for if l be even because we may need to reappraise (50). Should (49) be still possible for $p = 2$, then $\mathcal{S}$ is chosen as before with a like conclusion. But, if it be impossible, then clearly a is odd because b would be odd if a were even, whence we can find a solution of

$$A_2H_2 + B_2 \not\equiv 0, \bmod 2, \qquad aH_2 + b \equiv 2, \bmod 4,$$

and can thus produce a residue class H, $\bmod 2l_2$, for which

$$(A_2H + B_2, l_2) = 1, \qquad (aH + b, 2l_2) = 2.$$

By means of this residue class, we replace the numbers $n = n_1$ previously used in $an+b$ by the numbers $n_2 = H + 2ql_2$ to obtain the arithmetical progression $aH + b + 2aql_2$ for which $2 \leq (aH+b, 2al_2) \leq (b,a)(aH+b, 2l_2) = 2$ and thus $(aH+b, 2al_2) = 2$ and to which, therefore, Lemma 2.1 is applicable for the formation of a suitable sequence of n_2 of type $\mathcal{S}$. Once again, taking any value of $n = n_2$ for which (47) holds, we regain (48), in which μ is now obviously even.

The theorem follows quickly from the truth of (48) for the infinite sequences of n used therein. First,

$$2s = l(an + b) \pm \mu(A_2n + B_2)$$

so that choosing the minus sign in accord with (43) and the signs of A_2 and B_2, we have

$$s = \alpha n + \beta$$

for definite numbers α and β, where either $\alpha > 0$ or $\alpha = 0$, $\beta > 0$; these are integers if l be even but are otherwise quotients of integers divided by 2. From this, returning to (40) via (41), we find that

$$F(n) = l(an + b)\{l^2(an + b)^2 - 3l(an + b)(\alpha n + \beta) + 3(\alpha n + \beta)^2\}$$

for as many values of n as we wish. Thus there is the identity

$$F(x) = l(ax + b)\{l^2(ax + b)^2 - 3l(ax + b)(\alpha x + \beta) + 3(\alpha x + \beta)^2\},$$

from which it is clear that α and β are integers even when l is odd because $F(x)$ has integral coefficients. Consequently, along with (36), we see that

$$F(x) = \{l(ax + b) - (\alpha x + \beta)\}^3 + (\alpha x + \beta)^3 \tag{51}$$

identically, and we therefore have

Theorem 1. *Suppose that $F(x)$ is a cubic polynomial with integral coefficients with the property that $F(n)$ is equal to a sum of two positive integral cubes for all sufficiently large integers n. Then $F(x)$ is identically the sum of two cubes of polynomials with integral coefficients (in this case linear or constant that are both positive for sufficiently large values of x).*

5. Two cubes of either sign

Partially for its own interest and partially as a preparation for our consideration of general cubic polynomials $F(x_0, \dots, x_r)$ that are sums of two cubes, the next topic concerns what happens when we substitute for Hypothesis P the weaker

Hypothesis $\mathbf{P_1}$. *The conditions of Hypothesis P hold except that $F(n)$ is now merely assumed to be equal to a sum of two integral cubes of either sign.*

For reasons that will become clear in due course, this hypothesis is not quite strong enough to serve our purposes fully and we shall therefore add to it by assuming either

(i) $F(x)$ is not the cube of an integral linear form, or

(ii) the cubes in the representation of $F(n)$ are both non-zero,

although ultimately it will be obvious that (i) is stronger than (ii) when P_1 is given. Yet, until we have completed the first part of the demonstration by shewing that $F(x)$ is still reducible when P_1 is assumed, no cognizance of the additional suppositions need be taken.

Without losing any generality, we may clearly assume that the leading coefficient in $F(x)$ is positive so that $F(n) > 0$ for $n > n_0$. Thus in the assumed representation of $F(n)$ as $\xi^3 + \eta^3$ we see that $\xi + \eta > 0$ so that the number r in (1) is positive whereas s may be of either sign; in particular $s \le 0$ when $\eta \le 0$. Next, first assuming as at the beginning of section 3 that $F(x)$ is irreducible and then choosing a suitably large positive constant c_{20}, we take instead of $\Upsilon(X)$ the parallel sum $\Theta(X)$ that stems from the removal of the condition $s > 0$ in (6). Then, let us take $\Theta^{(1)}(X)$ and $\Theta^{(2)}(X)$ to be the respective contributions to $\Theta(X)$ due to the ranges

$$-c_{20}r \le s \le \frac{1}{2}r \qquad \text{and} \qquad s < -c_{20}r$$

so that $\Theta(X) = \Theta^{(1)}(X) + \Theta^{(2)}(X)$. An examination of the former sum $\Theta^{(1)}(X)$ reveals that the secondary inequality in (8) must give way to

$$r^2 - 3rs + 3s^2 \le \left\{ \frac{1}{4} + 3\left(c_{20} + \frac{1}{2} \right) \right\}^2 r^2 \tag{52}$$

with the implication that (9) is still valid provided that c_4 be turned into a sufficiently large constant c_{21}. The bound for $\Upsilon(X)$ being thus applicable to $\Theta^{(1)}(X)$, we find that

$$\Theta(X) = \Theta^{(2)}(X) + o(X) \tag{53}$$

in virtue of (33).

A different approach is needed for the sum $\Theta^{(2)}(X)$, the estimation of which begins with the observation that the opposite of (52) implies that (9) should be superseded by the inequalities

$$r \leq \gamma X, \qquad n \leq X,$$

in which $\gamma = \gamma(c_{20})$ can be taken to be a positive number as small as we please. Therefore

$$\Theta^{(2)}(X) = \sum_{r \leq \gamma X} \Theta_r^{(2)}(X), \tag{54}$$

where $\Theta_r^{(2)}(X)$ is the number of positive integers n up to X for which the equality

$$F(n) = rm$$

holds with m of the form $\frac{1}{4}r^2 + 3(\frac{1}{2}r - s)^2$. Here, as in previous arguments, n must belong to one of the $\rho(r)$ incongruent residue classes ν, $\bmod r$, for which $F(\nu) \equiv 0$, $\bmod r$, whence we write

$$\Theta_r^{(2)}(X) = \sum_{\substack{F(\nu) \equiv 0, \bmod r \\ 0 < \nu \leq r}} \Theta_{r,\nu}^{(2)}(X), \tag{55}$$

$\Theta_{r,\nu}^{(2)}$ being the contribution to $\Theta_r^{(2)}(X)$ due to the values of n that are congruent to ν, $\bmod r$.

The conditions of summation in $\Theta_{r,\nu}^{(2)}(X)$ not only imply (when non-empty) that n is restricted to a single residue class, $\bmod r$, but also that

$$F(n) \equiv r\left(\frac{1}{4}r^2 + 3\left(\frac{1}{2}r - s\right)^2\right), \bmod p, \tag{56}$$

for any prime p and, in particular, for any one that is subject to the conditions

$$p \nmid r, \qquad c_{22} < p \leq u, \tag{57}$$

where c_{22} is sufficiently large and $u = u(X, r)$ will be chosen suitably later. Let $S(r, p)$ be the number of incongruent solutions in n and s of (56) or, in other words, the number in n and σ of

$$4F(n) \equiv r^3 + 3r\sigma^2, \bmod p, \tag{58}$$

which by a well-known theorem due to Weil [15] is equal to

$$p + O\big(p^{\frac{1}{2}}\big) > \frac{1}{2}p$$

because of the obvious absolute irreducibility of

$$4F(n) - r^3 - 3r\sigma^2$$

as a polynomial, $\bmod p$, in n and σ. For each admissible value of $n, \bmod p$, in (58), there correspond two incongruent solutions in σ save when $4F(n) - r^3 \equiv 0, \bmod p$, in which case there is one solution $\sigma \equiv 0, \bmod p$ that occurs at most thrice. Therefore, for any prime p in the set given by (57), the number $T(r,p)$ of incongruent residue classes, $\bmod p$, to which n in (56) can belong is equal to

$$\frac{1}{2}S(r,p) + O(1) = \frac{1}{2}p + O\big(p^{\frac{1}{2}}\big). \tag{59}$$

The values of n that can occur in connection with the sum $\Theta^{(2)}_{r,\nu}(X)$ being restricted by the residue classes to various moduli in which they lie, their cardinality is most handily majorized by using the following ingenious theorem of Gallagher's [4] (see, for example, chapter 1 of our tract [7]).

Lemma 5.1. *If a set of positive integers not exceeding X include only representatives from at most $v(k) > 0$ residue classes for each prime power modulus k, then the number of integers in the set is at most*

$$\Big(\sum_{k\in T}\Lambda(k) - \log X\Big)\Big/\Big(\sum_{k\in T}\frac{\Lambda(k)}{v(k)} - \log X\Big) \tag{60}$$

whenever T is any finite set of moduli for which the denominator is positive.

In adopting this procedure, we follow the precedent of our work on power-free numbers [7, chapter 4], in which there is an application of the lemma in a somewhat similar vein.

The moduli k in the set T to be used in the estimation of $\Theta^{(2)}_{r,\nu}(X)$ are to be the prime power divisors of r and the primes p governed by (57). Then, by (59), the denominator in the appropriate form of (60) is

$$\begin{aligned}\sum_{k\,|\,r}\Lambda(k) + \sum_{\substack{c_{22}<p\le u\\ p\nmid r}}\frac{\log p}{T(r,p)} - \log X &= 2\sum_{\substack{c_{22}<p\le u\\ p\nmid r}}\frac{\log p}{p} + O\Big(\sum_p \frac{\log p}{p^{\frac{3}{2}}}\Big) - \log\frac{X}{r}\\ &\ge 2\log u - \sum_{p\,|\,r}\frac{\log p}{p} - \log\frac{X}{r} + O(1),\end{aligned}$$

which exceeds 1 if

$$\begin{aligned}u &= c_{23}\Big(\frac{X}{r}\Big)^{\frac{1}{2}}\exp\Big(\frac{1}{2}\sum_{p\,|\,r}\frac{\log p}{p}\Big)\\ &\le c_{23}\Big(\frac{X}{r}\Big)^{\frac{1}{2}}\prod_{p\,|\,r}\Big(1+\frac{\log p}{p}\Big) \le c_{23}\Big(\frac{X}{r}\Big)^{\frac{1}{2}}\sigma_{-\frac{1}{2}}(r)\end{aligned}$$

by some simple inequalities. The numerator in (60) being then not greater

$$\sum_{k\,|\,r}\Lambda(k)+\sum_{p\le u}\log p-\log X<2u-\log\frac{X}{r}<2u,$$

we deduce that

$$\Theta^{(2)}_{r,\nu}=O\biggl\{\biggl(\frac{X}{r}\biggr)^{\frac12}\sigma_{-\frac12}(r)\biggr\}$$

and hence that

$$\Theta^{(2)}(X)=O\biggl(X^{\frac12}\sum_{r\le\gamma X}\frac{\rho(r)\sigma_{-\frac12}(r)}{r^{\frac12}}\biggr)$$

by way of (54) and (55).

But, by Lemma 2.3 and partial summation,

$$\begin{aligned}\sum_{r\le y}\frac{\rho(r)\sigma_{-\frac12}(r)}{r^{\frac12}}&=\sum_{r'd\le y}\frac{\rho(r'd)}{r'^{\frac12}d^{\frac32}}=O\biggl(\sum_{r'\le y}\frac{\rho(r')}{r'^{\frac12}}\sum_{d}\frac{\rho(d)}{d^{\frac32}}\biggr)\\&=O\biggl(\sum_{r'\le y}\frac{\rho(r')}{r'^{\frac12}}\biggr)=O\bigl(y^{\frac12}\bigr),\end{aligned}$$

wherefore

$$\Theta^{(2)}(X)=O\bigl(\gamma^{\frac12}X\bigr)<\frac12X$$

if γ be chosen to be sufficient small, the constants implied by the O-notation being only dependent on $F(x)$. Hence from (53) we reach the inequality

$$\Theta(X)<\frac34X\qquad(X>X_0),$$

which, being inconsistent with Hypothesis P_1, means that we infer that $F(x)$ is not irreducible.

Our conclusions on the constitution of $F(x)$ are drawn by following closely the argument in section 4 provided that we assume one of the extra stipulations (i) or (ii) given below the statement of P_1. Remembering that the number s appearing in the analysis is no longer necessarily positive, let us first consider the situation where $F(x)$ is of the form $D(ax+b)^3$ as in (34). Then, in (35), $s\ne0$ by either (i) or (ii) because D cannot equal l^3 under the former condition, whence (35) holds with a non-zero value of l_1 (positive or negative) not exceeding $\frac12 l$. In the other case where (34) does not obtain it is obvious that we still have (51), in which neither cube vanishes for $x>x_0$. We therefore have demonstrated

Theorem 2. *Suppose $F(x)$ is a cubic polynomial with integral coefficients having the property that $F(n)$ is equal to the sum of two cubes for all sufficiently large integers n. Suppose also that either $F(x)$ is not the perfect cube of a linear integral binomial or that the cubes in the representation of $F(n)$ are both non-zero. Then $F(x)$ is identically equal to the sum of two cubes of non-zero polynomials with integral coefficients (in this case, linear or constant, having invariable signs for sufficiently large x).*

A final comment should be made on the treatments of the reducibility of $F(x)$ in section 2 and this section. At first sight it may seem incongruous that different types of sieve method should have been adopted for $\Theta^{(1)}(X)$ (or $\Upsilon(X)$) and $\Theta^{(2)}(X)$. But, underlying the differences between the two types of sum that are delineated by the sign of s and the size of r, there is the feature that $\Theta^{(1)}(X)$ is less demanding that $\Theta^{(2)}(X)$ in regard to the strength of the sieving needed but that it is more demanding in that its treatment cannot avoid the use of exponential sums. Since to overcome the harder aspects of both sums in a unified analysis would involve complications including the necessity of replacing Gallagher's method by the Selberg sieve, it is simpler to deal with each sum separately.

6. Polynomials in several variables that are a sum of two cubes

Going on to cubic polynomials in several variables, we generalize the Hypothesis P_1 of the previous section by enunciating

Hypothesis $\mathbf{P_2}$. *$F(x_0, \dots, x_r)$ is a cubic polynomial with integral coefficients that is not identically the cube of a linear polynomial and that has the property that it equals the sum of two integral cubes for all integral values of $x_0, \dots, x_r$.*

Our aim is to shew that under this hypothesis the polynomial $F(x_0, \dots, x_r)$ is identically the sum of two cubes of linear polynomials in $x_0, \dots, x_r$ that have integer coefficients. This being so, there are a number of simplifying assumptions and comments we should make before we embark on the main part of the proof. First, although we do not advert to this point again, it would be enough to assume that the second property in P_2 held merely for all sufficiently large values of $x_0, \dots, x_r$. Secondly, in the interests of clarity, we may suppose that each indeterminate x_i appears explicitly in the expression for $F(x_0, \dots, x_r)$ and then that $r \geq 1$ in virtue of Theorem 2. Also, it being obvious that the proposition to be established is invariant under transformations of the indeterminates by unimodular substitutions with integral coefficients, we may assume in the usual way that the coefficient a of the leading term ax_0^3 in $F(x_0, \dots, x_r)$ is non-zero (and indeed positive) by using, if necessary, relative prime integers $\alpha_0, \dots, \alpha_r$ for which $F(\alpha_0, \dots, \alpha_r) \neq 0$ and a substitution that takes $(\alpha_0, \dots, \alpha_r)$ into $(1, 0, \dots, 0)$. Indeed, this is just a part of a general principle, to which we shall have occasion to refer later, to the effect that any set of non-zero polynomials $\phi_1(y_0, \dots, y_s), \dots, \phi_u(y_0, \dots, y_s)$ is equivalent under a non-singular uni-

modular substitution with integral coefficients to a set of polynomials whose leading coefficients are non-zero.

In reflection of these remarks and our later needs we now decide on a change of notation and write

$$x_0 = \xi; \qquad (x_1, \dots, x_r) = (t_1, \dots, t_r) = \mathbf{t} \qquad (r \geq 1) \tag{61}$$

with the consequence that

$$F(\xi, \mathbf{t}) = a\xi^3 + l(\mathbf{t})\xi^2 + q(\mathbf{t})\xi + c(\mathbf{t}), \tag{62}$$

where, as the alphabetic representation suggests, $l(\mathbf{t})$, $q(\mathbf{t})$, $c(\mathbf{t})$ are polynomials in $t_1, \dots, t_r$ with integral coefficients that have degrees not exceeding two, three, or four. Initially the symbols ξ, t_i are indeterminates but, in accordance with standard practice, may also denote certain of their specializations in a manner to be described.

There are two cases to be considered, the first and easier being where F is a multiple — necessarily not by a perfect cube — of a perfect cube of a primitive linear polynomial. In this instance, for some number D that is not a perfect cube,

$$F(\xi, \mathbf{t}) = D(a^*\xi + l^*(\mathbf{t}))^3 = D(a^*\xi + l_1t_1 + \cdots + l_rt_r + l_{r+1})^3 \qquad (\mathrm{h.\,c.\,f.}(a^*, l_1, \dots, l_{r+1}) = 1) \tag{63}$$

and this, for any given integral $\mathbf{t}$ and all integers ξ, is equal to a sum of two integral cubes. In this, as we shall shew is possible, let us choose an integral $\mathbf{t}$ that has the property that

$$(a^*, l^*(\mathbf{t})) = 1. \tag{64}$$

Indeed, it being evident that we need only consider the case where $(l_1, \dots, l_{r+1}) = 1$, let $q = \mathrm{h.\,c.\,f.}(l_1, \dots, l_r)$ and infer first that $(q, l_{r+1}) = 1$ and that

$$l_1t_1 + \cdots + l_rt_r = q(l_1't_1 + \cdots + l_r't_r),$$

say, can take any integral value of the type qt by a suitable choice of $t_1, \dots, t_r$. Then to meet our requirement we only need to find t so that

$$l^*(\mathbf{t}) + l_{r+1} = qt + l_{r+1}$$

is incongruent to zero, modulis all prime factors p of a^*, this being done by taking $t \equiv 1, \mathrm{mod}\, p$, or $t \equiv 0, \mathrm{mod}\, p$, according as $p \,|\, l_{r+1}$ or $p \nmid l_{r+1}$ because in the former case $p \nmid q$. Taken with (64), the polynomial in (63) becomes an example of (34), whence, by the reasoning following the latter equation that is continued in section 5, we see that

$$D = D_1^3 + D_2^3$$

for non-zero integers D_1, D_2. Therefore in these circumstances

$$F(\xi, \mathbf{t}) = D_1^3(a^*\xi + l^*(\mathbf{t}))^3 + D_2^3(a^*\xi + l^*(\mathbf{t}))^3$$

in settlement of the first case.

In considering the second and more important case where (63) does not obtain we shall allow ξ to take any integer value but shall restrain $\mathbf{t}$ (when taken with integer components) to lie in a region $\mathcal{L} = \mathcal{L}(Q)$ (of integer vectors) defined by

$$\|\mathbf{t}\| \leq Q \tag{65}$$

for some large Q. Since part of the argument will relate to certain sub-sets of the region, it will be convenient to use the phrase 'almost all $\mathbf{t}$' to mean that $\mathbf{t}$ belongs to a sub-set $\mathcal{L}^*$ of $\mathcal{L}$ whose cardinality differs from that of $\mathcal{L}$ by $o(Q^r)$. Also, for future reference, we should mention that it is obvious that a set of type $\mathcal{L}^*$ must contain a representative of every residue class $\mathbf{a}$, mod λ, for any small modulus λ; thus the principle embodied in (64) is seen to extend to $\mathbf{t} \in \mathcal{L}^*$ by the replacement, if necessary, of the given $\mathbf{t}$ by one congruent to it, mod a^*. Consequently we readily establish the truth of the statement:

if $l^\dagger(\mathbf{t})$ be a linear polynomial with rational coefficients (independent of Q) that is an integer for almost all $\mathbf{t}$, then these coefficients are integers (66)

by using the positive integer d that makes $dl^\dagger(\mathbf{t})$ primitive. Furthermore, it may be helpful to remind the reader that the number of zeros in $\mathcal{L}$ of a non-identically zero polynomial with integral coefficients is $O(Q^{r-1})$.

It is easily verified that the condition that $F(\xi, \mathbf{t})$, as expressed in (62), have a triple repeated factor of the form $a(\xi + u)^3$ for a given integral $\mathbf{t}$ is that

$$3aq(\mathbf{t}) = l^2(\mathbf{t}), \qquad 27a^2c(\mathbf{t}) = l^3(\mathbf{t}),$$

which equations cannot both become identities when we are outside the first case. Consequently the number of $\mathbf{t}$ in $\mathcal{L}$ for which $F(\xi, \mathbf{t})$ has a triple repeated factor is $O(Q^{r-1})$ and therefore the opposite holds for almost all $\mathbf{t}$. Since, by hypothesis, $F(\xi, \mathbf{t})$ is a sum of two integral cubes, we deduce from Theorem 2 and the remarks before it that, for almost all $\mathbf{t}$, it is identically in ξ a sum of two cubes of non-proportional linear polynomials in ξ, or, in other words, that

$$F(\xi, \mathbf{t}) = \{B_0(\mathbf{t})\xi + B_1(\mathbf{t})\}^3 + \{C_0(\mathbf{t})\xi + C_1(\mathbf{t})\}^3, \tag{67}$$

where $B_i(\mathbf{t})$, $C_i(\mathbf{t})$ are integers depending on $\mathbf{t}$ and $B_0(\mathbf{t})C_1(\mathbf{t}) - C_0(\mathbf{t})B_1(\mathbf{t}) \neq 0$. From this, equating coefficients of ξ^3, we find the equation

$$B_0^3(\mathbf{t}) + C_0^3(\mathbf{t}) = a$$

having only a finite number E, say, of distinct solutions in $B_0(\mathbf{t})$, $C_0(\mathbf{t})$, one of which B_0, C_0, say, must occur in a sub-set $\mathcal{L}_1$ of $\mathcal{L}$ of values of $\mathbf{t}$ in a set of cardinality Q^r/E. Consequently, in completion of the first stage of the treatment, there emerges the relation

$$F(\xi, \mathbf{t}) = \{B_0\xi + B_1(\mathbf{t})\}^3 + \{C_0\xi + C_1(\mathbf{t})\}^3 \tag{68}$$

as an identity in ξ for $\mathbf{t} \in \mathcal{L}_1$, where

$$B_0C_1(\mathbf{t}) - C_0B_1(\mathbf{t}) \neq 0. \tag{69}$$

However, it remains to determine the forms of $B_1(\mathbf{t})$ and $C_1(\mathbf{t})$ in order to replace (68) by an identity in ξ and $\mathbf{t}$, to which end we shall have recourse to several lemmata.

First there is the familiar

Lemma 6.1. *A cubic polynomial in y having a Hessian with distinct linear factors is uniquely expressible (apart from order) in the form*

$$\lambda(y+\alpha)^3 + \mu(y+\beta)^3,$$

where $\alpha \neq \beta$.

For the proof, which can depend on linear recurrences, see any classical treatise on quantics or invariants (for example Salmon [11]).

The other two lemmata upon which we shall directly depend follow from two introductory ones, the first of which states a weak form of the Lang-Weil theorem on the solutions of congruences (see Schmidt [13, corollary 5C, page 213]).

Lemma 6.2. *Let $\psi(u_1, \dots, u_s)$ be an absolutely irreducible (non-constant) polynomial with integral coefficients. Then, for $p > p_0(\psi)$, the number $N(p)$ of incongruent solutions of the congruence*

$$\psi(u_1, \dots, u_s) \equiv 0, \bmod p,$$

does not exceed

$$(12/11)p^{s-1}.$$

The other initial result required is due to Bombieri and Pilá [1].

Lemma 6.3. *Let $\psi(u, v)$ be a polynomial of degree $d > 1$ with integer coefficients that is absolutely irreducible. Then the number of integral solutions of the equation $\psi(u, v) = 0$ for which $|u|, |v| \leq Q_1$ is $O\big(Q_1^{\frac{1}{d}+\varepsilon}\big)$, where the constants implied by the O-notation are independent of the coefficients in $\psi(u, v)$.*

From Lemma 6.2 we can deduce

Lemma 6.4. *Let $\mathcal{L} = \mathcal{L}(Q)$ be still defined as before through condition* (65) *and suppose $h(\mathbf{t})$ is a (given) polynomial with integral coefficients that is equal to a perfect square for more than E_1Q^r vectors $\mathbf{t}$ in $\mathcal{L}$, where E_1 is any (small) positive constant. Then $h(\mathbf{t})$ is identically equal to the square of a polynomial in $\mathbf{t}$ with integral coefficients.*

In this statement the word 'square' may be replaced by 'cube'.

The result is obvious if $h(\mathbf{t})$ be a constant. Otherwise, let us assume that $h(\mathbf{t})$ is not identically a multiple of a square of a polynomial with integral coefficients so that the polynomial

$$h(\mathbf{t}) - u^2 \tag{70}$$

would be absolutely irreducible. Then, choosing p_0 as in Lemma 6.2 when ψ therein is (70), let us take a sequence of consecutive primes $p_1 < p_2 < \cdots < p_w$ exceeding p_0 whose product Π is less than Q so w can be taken to be large. The number $M(Q)$ of $\mathbf{t}$ in $\mathcal{L}$ for which $h(\mathbf{t})$ is a perfect square is obviously not more than the number of $\mathbf{t}$ in $\mathcal{L}$ for which $h(\mathbf{t})$ is congruent to a square, mod Π, and therefore

$$M(Q) \le \left(\frac{2Q}{\Pi}\right)^r R(\Pi),$$

where $R(\Pi)$ is the number of incongruent $\mathbf{t}$, mod Π for which $h(\mathbf{t})$ is congruent to a square, modulis all prime divisors p of Π. To profit from this statement, let $N_1(p)$ and $N(p)$, respectively, be the number of incongruent solutions of $h(\mathbf{t}) \equiv 0$, mod p, and of (70) equated to zero, mod p, with the consequence that

$$N_1(p) = O(p^{r-1}) \qquad \text{and} \qquad N(p) \le (11/10)p^r \qquad (p > p_0)$$

by Lemma 6.2. Thus, since a soluble congruence of the type $u^2 \equiv m$, mod p, has two or one incongruent solutions according as $p \nmid m$ or $p \mid m$, we would deduce that

$$M(Q) \le \left(\frac{2Q}{\Pi}\right)^r \frac{1}{2^w} \prod \{N_1(p_i) + N(p_i)\} < \left(\frac{3}{5}\right)^w (2Q)^r,$$

which is less than $E_1 Q^r$. Hence, the assumption being inconsistent with what we were given, we deduce that $h(\mathbf{t}) = m h_1^2(\mathbf{t})$ for some integer m, which is seen to be a perfect square by a selection of $\mathbf{t}$ for which $h(\mathbf{t})$ itself is. This completes the proof of the first part; the second part is demonstrated similarly except that we should restrict the primes p to be congruent to 1, mod 3.

As stated in the introduction, propositions of the above type have a long history. But, for the result as stated, the proof chosen seems to be the shortest.

Finally, from Lemma 6.3, we can obtain our final ancillary result, in the statement of which $\mathcal{L} = \mathcal{L}(Q)$ has the same meaning as in Lemma 6.4.

Lemma 6.5. *Suppose that $f(\mathbf{t})$ and $g(\mathbf{t})$ are mutually prime non-zero polynomials and that $f(\mathbf{t})/g(\mathbf{t})$ is a (determinate) integer for more than $E_1 Q^r$ vectors $\mathbf{t}$ in $\mathcal{L}$, where E_1 is any (small) positive constant. Then $g(\mathbf{t})$ is identically equal to a non-zero constant.*

Assume that the degree of $g(\mathbf{t})$ is greater than zero and consider first the case where $f(\mathbf{t})$ is the constant $G \neq 0$. Then in looking at the underlying indeterminate equation

$$f(\mathbf{t}) = u g(\mathbf{t}) \qquad (g(\mathbf{t}) \neq 0) \tag{71}$$

in $\mathbf{t} \in \mathcal{L}$ and u, we see in this case that u divides G and has $O(1)$ possible values. Hence $g(\mathbf{t})$ can only assume a finite number of determinations G_1, say, while the number of solutions of $g(\mathbf{t}) = G_1$ in $\mathcal{L}$ is $O\left(Q^{r-1}\right)$. The total number of relevant solutions of (71) in $\mathbf{t}$ being less than what was stated, we deduce that $g(\mathbf{t})$ is a non-zero constant.

To avoid awkward notational conventions we restrict our attention to the case $r > 1$ when considering the situation where $f(\mathbf{t})$ is of degree $\rho \geq 1$, it then being clear how the easier case $r = 1$ should be treated along parallel lines; indeed, the latter could be handled in a very elementary way without the use of Lemma 6.3. First, by an introductory comment in this section, we may suppose that $f(\mathbf{t})$ and $g(\mathbf{t})$ have been so prepared that their leading coefficients a_0, b_0 are non-zero provided that Q and E_1 be adjusted through their being affected by numerical multipliers. Thus, changing for convenience the notation by expressing $\mathbf{t}$ as

$$(t, t_2, \dots, t_r) = (t, \mathbf{t}_2),$$

we may write

$$f(\mathbf{t}) = f_{\mathbf{t}_2}(t) = a_0 t^\rho + a_1(\mathbf{t}_2) t^{\rho-1} + \cdots + a_\rho(\mathbf{t}_2),$$
$$g(\mathbf{t}) = g_{\mathbf{t}_2}(t) = b_0 t^\sigma + b_1(\mathbf{t}_2) t^{\sigma-1} + \cdots + b_\sigma(\mathbf{t}_2),$$

which qua polynomials in t have a resultant $R(\mathbf{t}_2)$ that is subject to an identity of the type

$$h_1(\mathbf{t}) f_{\mathbf{t}_2}(t) + h_2(\mathbf{t}) g_{\mathbf{t}_2}(t) = R(\mathbf{t}_2)$$

containing polynomials $h_1(\mathbf{t})$, $h_2(\mathbf{t})$ of degrees less than σ, ρ in $\mathbf{t}$. Here $R(\mathbf{t}_2)$ is not identically zero, since otherwise $f(\mathbf{t})$ and $g(\mathbf{t})$ would have a non-constant factor in common. Hence, save for $O(Q^{r-2})$ determinations of $\mathbf{t}_2$ for which $R(\mathbf{t}_2) = 0$ and $\|\mathbf{t}_2\| \leq Q$, the polynomials $f(\mathbf{t})$ and $g(\mathbf{t})$ are relatively prime apart from numerical factors depending on a_0 and b_0. We then return to (71) and, in counting the number of its relevant solutions, ignore those appertaining to the exceptional set of $\mathbf{t}_2$ above because they correspond to a sub-set of $\mathcal{L}$ having cardinality $O(Q^{r-1})$.

Since, for any integer G_2, the indeterminate equation $g(\mathbf{t}) = G_2$ has $O(Q^{r-1})$ solutions in $\mathcal{L}$, the relevant solutions of (71) for which $|g(\mathbf{t})| \leq Q^{\frac{1}{2}}$ are in number $O(Q^{r-\frac{1}{2}})$ and may therefore be also ignored. But, for the other solutions, let us rephrase (71) as

$$f_{\mathbf{t}_2}(t) - u g_{\mathbf{t}_2}(t) = 0 \tag{72}$$

and, for each eligible $\mathbf{t}_2$, regard it as an equation in integers u, t that are circumscribed by the obvious inequalities

$$|u| < Q^{-\frac{1}{2}} f_{\mathbf{t}_2}(t) < c Q^{\rho-\frac{1}{2}}, \qquad |t| \leq Q.$$

Here the defining polynomial is not only absolutely irreducible by the co-primality of $f_{\mathbf{t}_2}(t)$ and $g_{\mathbf{t}_2}(t)$ but also of degree not less that 2 or ρ according as $\rho = 1$ or $\rho > 1$.

Hence, by Lemma 6.3, the number of relevant solutions of (72) is $O(Q^{\frac{1}{2}+\varepsilon})$ if $\rho = 1$ but $O(Q^{\frac{1}{\rho}(\rho-\frac{1}{2})+\varepsilon}) = O(Q^{1-\frac{1}{2\rho}+\varepsilon})$ if $\rho > 1$, whence summing over $\mathbf{t}_2$, we get $O(Q^{r-\frac{1}{2\rho}+\varepsilon})$ solutions in $\mathbf{t}$ in contradiction with the data supplied. This completes the proof for the case $\rho \geq 1$.

Being ready to take account of equation (68), we begin with the case where one (but not both) of B_0, C_0 is zero and choose, for example, that where $B_0 = 0$. Then, comparing the consequential equation

$$F(\xi, \mathbf{t}) = C_0^3\xi^3 + 3C_0^2C_1(\mathbf{t})\xi^2 + 3C_0C_2^2(\mathbf{t})\xi + C_1^3(\mathbf{t}) + B_1^3(\mathbf{t})$$

with (62) when $\mathbf{t} \in \mathcal{L}_1$, we deduce that

$$3C_0^2C_1(\mathbf{t}) = l(\mathbf{t})$$

and then that

$$B_1^3(\mathbf{t}) = c(\mathbf{t}) - \frac{l^3(\mathbf{t})}{27C_0^6} \neq 0.$$

by (69). Being of degree not exceeding three and being a perfect cube for all $\mathbf{t} \in \mathcal{L}_1$, the polynomial on the right is seen through Lemma 6.4 to be identically a perfect cube of a rational multiple $\lambda w_1(\mathbf{t})$ of a primitive linear polynomial. Thus

$$F(\xi, \mathbf{t}) = \{\lambda w_1(\mathbf{t})\}^3 + \{C_0\xi + w_2(\mathbf{t})\}^3,$$

where $w_2(\mathbf{t})$ is also a linear polynomial, and this, being true for $\mathbf{t} \in \mathcal{L}_1$, is actually an identity. Since, by (67) and the uniqueness theorem of Lemma 6.1, $\lambda w_1(\mathbf{t})$ and $w_2(\mathbf{t})$ are integers for almost all $\mathbf{t}$, we deduce from statement (66) that $\lambda w_1(\mathbf{t})$ and $w_2(\mathbf{t})$ have integral coefficients and thus obtain what we need in this instance.

Going on to the case where $B_0, C_0 \neq 0$, we observe that $F(\xi, \mathbf{t})$ as a cubic in ξ has a Hessian that is both

$$\{B_0C_1(\mathbf{t}) - C_0B_1(\mathbf{t})\}^2\{B_0\xi + B_1(\mathbf{t})\}\{C_0\xi + C_1(\mathbf{t})\} \tag{73}$$

and of the form

$$q_1(\mathbf{t})\xi^2 + c_1(\mathbf{t})\xi + b_1(\mathbf{t}) \qquad (q_1(\mathbf{t}) \neq 0) \tag{74}$$

for $\mathbf{t} \in \mathcal{L}_1$ because of (68) and (62), where the degrees of $q_1(\mathbf{t})$, $c_1(\mathbf{t})$, and $b_1(\mathbf{t})$ do not exceed two, three, and four, respectively. Consequently, for $\mathbf{t} \in \mathcal{L}_1$,the quadratic (74) breaks up into rational linear factors and therefore its discriminant

$$c_1^2(\mathbf{t}) - 4q_1(\mathbf{t})b_1(\mathbf{t})$$

is a perfect square (but not zero by what has gone before). Hence, by Lemma 6.4, this discriminant is identically a perfect square and (74) may be thrown into the form

$$u(\mathbf{t})\{v_0(\mathbf{t})\xi + v_1(\mathbf{t})\}\{w_0(\mathbf{t})\xi + w_1(\mathbf{t})\}, \tag{75}$$

where $v_0(\mathbf{t})$, $v_1(\mathbf{t})$ and $w_0(\mathbf{t})$, $w_1(\mathbf{t})$ are pairs of relatively prime polynomials with integer coefficients. Comparing the factors in (73) and (75) by ordering them appropriately with a suitable notation, we then deduce that, for $\mathbf{t}$ in a set $\mathcal{L}_2$ consisting of not less than half the number of members of $\mathcal{L}_1$, the factors $B_0\xi + B_1(\mathbf{t})$ and $C_0\xi + C_1(\mathbf{t})$ are proportional to $v_0(\mathbf{t})\xi + v_1(\mathbf{t})$ and $w_0(\mathbf{t})\xi + w_1(\mathbf{t})$, respectively.

First, if $v_1(\mathbf{t}) = 0$ identically, then $v_0(\mathbf{t})$ is a non-zero constant. Yet, if $v_1(\mathbf{t})$ and therefore $B_0 v_1(\mathbf{t})$ be not identically zero, then

$$\frac{B_0 v_1(\mathbf{t})}{v_0(\mathbf{t})} = B_1(\mathbf{t})$$

is always an integer in $\mathcal{L}_2$, whence $v_0(\mathbf{t})$ is still identically a non-zero constant by Lemma 6.5. Since similar conclusions about the other factor in the Hessian may be drawn, we deduce, for $\mathbf{t} \in \mathcal{L}_2$ in the first place and hence identically, the formula

$$F(\xi, \mathbf{t}) = \{B_0\xi + \upsilon(\mathbf{t})\}^3 + \{C_0\xi + w(\mathbf{t})\}^3$$

containing polynomials $\upsilon(\mathbf{t})$, $w(\mathbf{t})$ with rational coefficients. But, if $\upsilon^*(\mathbf{t})$, $w^*(\mathbf{t})$ be the components of $\upsilon(\mathbf{t})$ and $w(\mathbf{t})$ of degree exceeding one, then, since $F(\xi, \mathbf{t})$ is cubic and $B_0 \neq -C_0$,

$$\upsilon^{*3}(\mathbf{t}) + w^{*3}(\mathbf{t}) = 0, \qquad B_0\upsilon^{*2}(\mathbf{t}) + C_0 w^{*2}(\mathbf{t}) = 0$$

and hence $\upsilon^*(\mathbf{t}) = -w^*(\mathbf{t}) = 0$, the polynomials $\upsilon(\mathbf{t})$ and $w(\mathbf{t})$ being linear. Finally, by (67) and the uniqueness theorem of Lemma 6.1, $\upsilon(\mathbf{t})$ and $w(\mathbf{t})$ are integers for all $\mathbf{t}$ and therefore have integral coefficients in virtue of statement (66).

Reverting to the original notation associated with (61), we have thus obtained

Theorem 3. *Let $F(x_0, \ldots, x_r)$ be a cubic polynomial with (rational) integral coefficients that is not identically the cube of a linear polynomial with integral coefficients and that has the property that it equals the sum of two perfect cubes for all integral values $x_0, \ldots, x_r$. Then $F(x_0, \ldots, x_r)$ is identically equal to the sum of two cubes of linear polynomials in $x_0, \ldots, x_r$ with integral coefficients.*

References

[1] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. **59** (1989), no. 2, 337–357.

[2] H. Davenport, D. J. Lewis, and A. Schinzel, *Quadratic Diophantine equations with a parameter*, Acta Arith. **11** (1965/1966), 353–358.

[3] P. Erdös, *On the sum* $\sum_{k=1}^{x} d(f(k))$, J. London Math. Soc. **27** (1952), 7–15.

[4] P. X. Gallagher, *A larger sieve*, Acta Arith. **18** (1971), 77–81.

[5] C. Hooley, *On the representations of a number as the sum of two cubes*, Math. Z. **82** (1963), 259–266.

[6] ———, *On the distribution of the roots of polynomial congruences*, Mathematika **11** (1964), 39–49.

[7] ———, *Applications of sieve methods to the theory of numbers*, Cambridge Tracts in Mathematics, vol. 70, Cambridge University Press, Cambridge, 1976.

[8] ———, *On power-free numbers and polynomials*, I, J. Reine Angew. Math. **293/294** (1977), 67–85.

[9] T. Nagell, *Introduction to Number Theory*, John Wiley & Sons Inc., New York, 1951.

[10] G. Pólya and G. Szegő, *Aufgaben und Lehrsätze aus der Analysis*, II: *Funktionentheorie, Nullstellen, Polynome Determinanten, Zahlentheorie*, 4th ed., Heidelberger Taschenbücher, vol. 74, Springer-Verlag, Berlin, 1971.

[11] G. Salmon, *Lessons introductory to the modern higher algebra*, Dublin, 1885.

[12] A. Schinzel, *On the relation between two conjectures on polynomials*, Acta Arith. **38** (1980/81), no. 3, 285–322.

[13] W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, vol. 536, Springer-Verlag, Berlin, 1976.

[14] J. D. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc. (N.S.) **12** (1985), no. 2, 183–216.

[15] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. et Ind. **1041** (1948).

[16] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proc. London Math. Soc. (2) **21** (1922), 235–255.