Proc. Indian Acad. Sci. (Math. Sci.), Vol. 111, No. 3, August 2001, pp. 249–262.

On totally reducible binary forms: I

C HOOLEY

School of Mathematics, Cardiff University, Senghennydd Road, PO Box 926, Cardiff CF24 4YH, UK

MS received 18 October 2000; revised 7 February 2001

Abstract. Let $\nu(n)$ be the number of positive numbers up to a large limit n that are expressible in essentially more than one way by a binary form f that is a product of $\ell > 2$ distinct linear factors with integral coefficients. We prove that

$$\nu(n) = O\left(n^{2/\ell - \eta_\ell + \epsilon}\right),$$

where

$$\eta_\ell = \begin{cases} 1/\ell^2, \text{ if } \ell = 3, \\ (\ell - 2)/\ell^2(\ell - 1), \text{ if } \ell > 3, \end{cases}$$

thus demonstrating in particular that it is exceptional for a number represented by f to have essentially more than one representation.

Keyword. Binary forms.

1. Introduction

In this publication and its sequel we shall fulfil the undertaking given in our earlier paper [3] to resolve the following problems for binary forms f of degree $\ell > 2$ that are totally reducible as a product of ℓ (disjoint) linear factors with integral coefficients:

(i) to find an asymptotic formula for the number $\Upsilon(n) = \Upsilon_\ell(n)$ of positive integers that are expressible by f and do not exceed n, each such integer being counted just once regardless of multiplicity of representations (no generality is lost by debarring negative numbers because they can be treated by changing the sign of one of the linear factors in f);

(ii) to find an upper bound for the number $\nu(n) = \nu_\ell(n)$ of such integers that are represented in essentially more than one way.

We thus shall extend to a special class of binary forms of arbitrary degree the results obtained for cubics and certain other binary forms in former papers and, in particular, [3], to the last of which the reader is referred for a history of the problem and the relevant citations.

In interpreting the second quest, on which the first will be seen to depend, we must anticipate a later discussion by saying that representations of a number by the form are regarded as being inherently distinct if they be not associated with each other in an obvious way through an automorphic of the form. With this appreciation, we shall shew here that

$$\nu(n) = O\left(n^{2/\ell - \eta_\ell + \epsilon}\right), \tag{1}$$

where

$$\eta_\ell = \begin{cases} 1/\ell^2, \text{ if } \ell = 3, \\ (\ell-2)/\ell^2(\ell-1), \text{ if } \ell > 3, \end{cases}$$

from which it will be easily demonstrated that it is extremely rare for a number representable by f to be represented in essentially more than one way.

The derivation from this result of an asymptotic formula for $\Upsilon(n)$ principally depends on the properties of the automorphics of the form. We therefore reserve the treatment of item (i) for a second paper, especially as an exhaustive treatment of the structure of the automorphics occupies some space, is in itself an interesting study, and involves ideas that are somewhat alien to those used in the present work. Suffice it then for the time being to say that we shall ultimately obtain an asymptotic formula of the type

$$\Upsilon(n) \sim A(f)n^{2/\ell}, \quad (A(f) > 0)$$

with a remainder term similar to the right-hand side of (1).

We should mention that the advantage of our present methods – in contrast with those often used in problems of this type – is that they are also applicable to an inhomogeneous situation in which the subject of study is a completely reducible polynomial of degree ℓ consisting of factors of the type $hx+ky+q$. It is hoped to give an account of this extension to our work in due course.

2. Notation and conventions

As is often the case in the algebra of substitutions as applied to forms or quantics, each symbol for a variable therein will denote an indeterminate on some occasions and a specialization of this on other occasions. With this agreement, when not denoting indeterminates, r, s, ρ, σ are integers and m, μ with or without distinguishing marks are non-zero integers; p, ϖ are positive prime numbers. The letters $A_1, A_2, \ldots$ denote suitable positive constants depending at most on the form f under consideration; ϵ is an arbitrarily small positive number that is not necessarily the same at each occurrence; the constants implied by the O-notation are of type A_i save when they may also depend on ϵ.

Since negative integers may frequently occur, we should mention that they may be moduli in congruences. The terms size, magnitude, modulus are used as synonyms for absolute value when applied to real numbers. The notation (h, k) indicates the positive highest common factor (when defined) of integers h, k save when it designates a point with coordinates h, k; $d(m)$ is the number of positive divisors of m, while $d_r(m)$ is the number of ways expressing $|m|$ as a product of r positive factors.

3. Prolegomena

Being totally reducible over the rationals with no repeated factors, the binary form $f = f(x, y)$ of degree $\ell \geq 3$ under consideration is expressed as

$$\prod_{1\leq i\leq \ell}(h_i x + k_i y) = \prod_{1\leq i\leq \ell} L_i(x, y), \text{ say}, \tag{2}$$

where the coefficients of the linear forms $L_i(x, y)$ are integers and where, even apart from order, there is a slight but acceptable ambiguity in their definitions when f is imprimitive.

Of the invariants of the form, the only one that will be needed is the discriminant

$$D = D(f) = \prod_{1 \le i < j \le \ell} \left(h_i k_j - h_j k_i \right)^2 > 0, \tag{3}$$

which has the familiar property that, if $f(x, y)$ be transformed into $F(X, Y)$ by a substitution of modulus M, then

$$D(F) = M^{\ell^2 - \ell} \, D(f). \tag{4}$$

Also, since our investigation only concerns the representations of numbers by f without regard to the size of the variables in f, we may equally well work with any form f' equivalent to f through a rational integral substitution

$$x = \alpha X + \beta Y, \;\; y = \gamma X + \delta Y \tag{5}$$

with modulus

$$\alpha\delta - \gamma\beta = 1. \tag{6}$$

This means, in particular, that we may certainly assume that

$$h_1, h_2, \ldots, h_\ell \neq 0 \tag{7}$$

because[1], in the opposite instance, having chosen relatively prime numbers α, γ and then β, δ to satisfy $f(\alpha, \gamma) \neq 0$ and (6), we find through (5) a form with non-zero leading coefficient $f(\alpha, \gamma)$ that is equivalent to f.

Closely associated with our study of the representations by $f(x, y)$ of positive numbers up to a large limit n, the curve $C = C(n)$ defined by the equation

$$f(x, y) = n \tag{8}$$

will be encountered together with its asymptotes

$$L_1(x, y) = 0, \ldots, L_\ell(x, y) = 0, \tag{9}$$

which both here and in our second paper will play a not unimportant role in the elucidation of lattice point problems involving regions bounded by $C(n)$. Forming 2ℓ semi-infinite rays emanating from the origin, these asymptotes divide the plane into 2ℓ semi-infinite domains, in each of which $f(x, y)$ has a constant sign opposite to that pertaining to its neighbours. Moreover, from an examination of the configuration formed by (8) and (9), it would be foreseen that the major influence on our situation would be exerted by those x and y having absolute values not substantially larger than $n^{1/\ell}$, which expectation prompts us at once to write

$$N = n^{1/\ell} \tag{10}$$

for notational convenience. Next, elaborating on this line of thought analytically (a geometrical approach is more intuitive but harder to describe), we note by linear relationships that, if

$$\max_{1 \le i \le \ell} \left| L_i(x, y) \right| = L_u(x, y) = Q > 0 \tag{11}$$

[1] With a little more effort we can shew that we may suppose, in addition, that $k_1, \ldots, k_\ell \neq 0$.

for integer values of x and y, then we always have

$$|x|, |y| < A_1 Q. \tag{12}$$

Also, more significantly, if here

$$Q > A_2 N \tag{13}$$

for a sufficiently large positive constant A_2 and $f(x, y)$ obey the usually assumed inequality $0 < f(x, y) \leq n$, we see first that at least one form $L_\nu(x, y)$ for $\nu \neq u$ has magnitude not less than 1 and not greater than

$$(n/Q)^{1/(\ell-1)} < A_2^{-1/(\ell-1)} N < A_2^{-\ell/(\ell-1)} Q \tag{14}$$

and then deduce from linear relationships and (11) that this form $L_\nu(x, y)$ is unique, all other forms $L_i(x, y)$ having magnitudes greater then $A_3 Q$. Hence $A_3^{\ell-1} Q^{\ell-1} < n$ so that

$$Q < A_4 n^{1/(\ell-1)}, \tag{15}$$

while also the bound (14) is improved to

$$|L_\nu(x, y)| < \frac{n}{A_3^{\ell-1} Q^{\ell-1}} = \frac{A_5 n}{Q^{\ell-1}}. \tag{16}$$

Some amplification of an introductory remark about the automorphics of the form is needed at once even though a full examination of their structure will be delayed until our second paper. Let now

$$x = \alpha X + \beta Y, \ y = \gamma X + \delta Y \tag{17}$$

be a rational automorphic of f, namely, a substitution with rational coefficients $\alpha, \beta, \gamma, \delta$ with the property that $f(x, y) = f(X, Y)$ and, as we confirm from (4), the consequencial property that its modulus $\alpha\delta - \gamma\beta$ is equal to ± 1. Points $(x, y), (X, Y)$ with *integral* coordinates that are connected by means of an automorphic of type (17) will be said to be *associated*, the property of association being denoted by $(x, y) \simeq (X, Y)$. Then, since associated points give rise to linearly connected representations of the same number, we shall agree that representations of a number as $f(x, y)$ and $f(x', y')$ are deemed *essentially different* if $(x, y) \simeq (x', y')$. Thus an unmistakable meaning has been attached to $\nu(n)$, to whose estimation we now attend.

4. The sum $T(n)$ and the equation $m F(m, s) = \mu G(\mu, \sigma)$

The treatment depends on an analysis of the sum

$$T(n) = \sum_{\substack{0 < f(r,s) = f(\rho,\sigma) \leq n \\ (r,s) \not\simeq (\rho,\sigma)}} 1, \tag{18}$$

through which $\nu(n)$ is bounded by the obvious inequality

$$\nu(n) \leq T(n). \tag{19}$$

First, to dissect the sum into parts that can be appropriately assessed, let $T_1(n)$ be that portion of $T(n)$ that is yielded by values of r, s, ρ, σ in the conditions of summation for which a linear factor of maximal size in the constituents of the equation

$$f(r,s) = \prod_{1\le i\le \ell} L_i(r,s) = \prod_{1\le j\le \ell} L_j(\rho,\sigma) = f(\rho,\sigma)$$

occurs on the left. Then, allowing $T_1(n, M)$ to denote the contribution to $T_1(n)$ corresponding to values of r, s, ρ, σ for which the size of this maximal linear factor lies between M inclusive and $2M$ exclusive, we have

$$T(n) \le 2T_1(n)$$

and complete the first phase of the calculations by deducing that

$$T(n) \le 2\sum_i T_1(n, M_i), \tag{20}$$

in which

$$M_i = 2^i \qquad (i \ge 0) \tag{21}$$

is less than

$$A_4 n^{1/(\ell-1)} \tag{22}$$

by (15).

In further preparation for the estimation of $T(n)$ we examine the solutions of the indeterminate equation

$$f(r,s) = f(\rho,\sigma) \tag{23}$$

that are constrained by the conditions

$$L_u(r,s) = m, \qquad L_\nu(\rho,\sigma) = \mu \tag{24}$$

for given subscripts u, ν and non-zero integers m, μ. For this purpose, recalling (7), we employ the substitutions[2]

$$m = h_u r + k_u s, \qquad s = s, \tag{25}$$

$$\mu = h_\nu \rho + k_\nu \sigma, \qquad \sigma = \sigma, \tag{26}$$

to transform (23) into

$$\frac{m}{h_u^{\ell-1}} \prod_{i\ne u} \left\{ h_i m + \left(h_u k_i - h_i k_u\right) s \right\} = \frac{\mu}{h_\nu^{\ell-1}} \prod_{j\ne \nu} \left\{ h_j \mu + \left(h_\nu k_j - h_j k_\nu\right) \sigma \right\}, \tag{27}$$

which equation for brevity we express as either

$$mF(m,s) = \mu G(\mu,\sigma) \tag{28}$$

or

$$mF(m,s) - \mu G(\mu,\sigma) = 0, \tag{29}$$

[2] Remember the remarks in §2 about entities appearing in linear transformations. We should also comment that it would be pendantic and unhelpful here to introduce symbols s', σ' to substitute for s, σ in (27) and in the left sides of the right hand members of (25) and (26).

where $F(m,s) = F_u(m,s)$ and $G(\mu,\sigma) = G_\nu(\mu,\sigma)(= F_\nu(\mu,\sigma))$ are, respectively, of exact degree $\ell - 1$ in s and σ.

Needing to know when the curve defined by (27) for given non-zero integer values of m and μ is irreducible over $\mathbb{Q}$, we set

$$s = ms',\ \sigma = \mu\sigma',\ \lambda = (m/\mu)^\ell \neq 0$$

to form the equivalent curve

$$\lambda F(1,s') - G(1,\sigma') = 0, \tag{30}$$

which is certainly irreducible (indeed absolutely irreducible) when its projective completion

$$\lambda F(z,s') - G(z,\sigma') = 0$$

is non-singular and hence when the simultaneous equations

$$\frac{\partial F(z,s')}{\partial s'} = 0, \quad \frac{\partial G(z,\sigma')}{\partial \sigma'} = 0, \quad \lambda\frac{\partial F(z,s')}{\partial z} - \frac{\partial G(z,\sigma')}{\partial z} = 0$$

have no non-zero solution. But, if $z = 0$, the first two equations only hold when $s' = \sigma' = 0$, whereas otherwise, since $F(z,s')$ and $G(z,\sigma')$ are each products of real distinct factors, they are only satisfied when $s'/z, \sigma'/z$ each take $\ell - 2$ real values, each combination of which determines λ through the last equation because neither both $\partial F/\partial s',\ \partial F/\partial z$ nor both $\partial G/\partial\sigma', \partial G/\partial z$ can (non-trivially) simultaneously vanish. Thus reducible curves of type (30) answer to at most $(\ell-2)^2$ values of λ, and we therefore infer that (29) can only be reducible if

$$Bm = C\mu \tag{31}$$

for one of $O(1)$ sets of relatively prime (bounded) non-zero integers $B = B_{u,\nu},\ C = C_{u,\nu}$.

Of special importance is the case where the left side of (29) has a rational linear factor in s, σ, in which event for some pair B, C the left side of the corresponding equation (30) with $\lambda = (C/B)^\ell$ contains a linear factor $s' = D\sigma' + E$ with rational coefficients $D \neq 0$ and E that do not depend on m and μ. In this situation, we deduce from (31) that (28) holds identically whenever

$$Bs = Bms' = C\mu s' = CD\mu\sigma' + CE\mu = CD\sigma + CE\mu$$

and hence that the rational substitution

$$Bs = CD\sigma + CE\mu,\ Bm = C\mu$$

transforms $mF(m,s)$ into $\mu G(\mu,\sigma)$. Therefore, compounding this substitution with (26) and the inverse of (25) in the obvious order, we are provided with a rational automorphic of f that takes r, s into ρ, σ, whence any solutions of (29) arising in this way flow from associated points (r,s), (ρ,σ) and are of a type not counted in $T(n)$ and its constituent parts.

In combination with the special features just identified, the main instrument in our treatment of equation (29) is an important theorem due to Bombieri and Pila [1] that we state here as follows.

Lemma 1. *Let $\Psi(\xi, \eta)$ be an irreducible polynomial of degree δ with rational coefficients. Then the number of solutions of $\Psi(\xi, \eta) = 0$ in integers of size not exceeding z is*

$$O\left(z^{(1/\delta)+\epsilon}\right) \qquad (z \geq 1),$$

where the constants implied by the O-notation are independent of the coefficients of Ψ.

Proved by Bombieri and Pila when the condition of absolute irreducibility is imposed, the result of the lemma remains true if $\Psi(\xi, \eta)$ be irreducible but not absolutely irreducible because then any integer solution is a zero of an absolutely irreducible factor of $\Psi(\xi, \eta)$ of the form

$$\omega_1\psi_1(\xi, \eta) + \cdots + \omega_e\psi_e(\xi, \eta) \quad (\psi_i(\xi, \eta)\epsilon\mathbb{Q}[\xi, \eta]),$$

where $\omega_1, \ldots, \omega_e$ is a basis of the field of degree $e > 1$ over which the factor is defined. In fact the zeros of this are the common zeros of the system

$$\psi_1(\xi, \eta), \ldots, \psi_e(\xi, \eta),$$

which belong to a variety of dimension zero and limited degree since clearly $\psi_1, \ldots, \psi_e$ have no common factor. This confirms our extension of the Bombieri–Pila theorem in the context of the present work.

For the case $\ell = 3$ we shall need to augment our armoury with an elementary estimate that is sharper than Lemma 1 when $\Psi(\xi, \eta)$ is a special type of quadratic. This is as follows.

Lemma 2. *Let*

$$\Psi(\xi, \eta) = a_1\xi^2 + b_1\xi + a_2\eta^2 + b_2\eta + c \quad (a_1, a_2 \neq 0)$$

be an irreducible quadratic polynomial with rational coefficients having bounded denominators and size not exceeding z^{A_7}. Then the number of zeros of $\Psi(\xi, \eta)$ of size not exceeding z is $O(z^\epsilon)$ for $z \geq 1$.

Supposing first that $\Psi(\xi, \eta)$ is absolutely irreducible and noting that we may restrict attention to the case where it has integer coefficients, multiply it by $4a_1a_2$ to transform it into

$$a_2\left(2a_1\xi + b_1\right)^2 + a_1\left(2a_2\eta + b_2\right)^2 - \left(a_2b_1^2 + a_1b_2^2 - 4a_1a_2c\right)$$

with the implication that $a_2b_1^2 + a_1b_2^2 - 4a_1a_2c \neq 0$. Hence, since the solutions of $\Psi(\xi, \eta) = 0$ are contained in those of an equation of the type

$$a_3X^2 + a_4Y^2 = a_2b_1^2 + a_1b_2^2 - 4a_1a_2c,$$

we deduce that the solutions to be counted have cardinality

$$O\left\{d\left(a_2b_1^2 + a_1b_2^2 - c\right)\log 2z\right\} = O\left(z^\epsilon\right)$$

by a familiar application of the theory of quadratic forms as used for example in our paper [2].

The case where Ψ is irreducible but not absolutely irreducible is catered for by the argument in the proof of Lemma 1 or, alternatively, is easily handled *a priori* in the present framework by obvious reasoning.

5. Estimation of $T(n)$ and the first theorem

In treating the sum $T(n)$ in (17), which we now rejoin, we shall first primarily address the case where $\ell > 3$ and shall delay until later a modified argument for $\ell = 3$ that largely depends on Lemma 2 instead of Lemma 1, although it should be stressed that nothing in the earlier stages of the reasoning is actually invalid for the latter case.

Having indicated the sphere of operation, we first suppose that

$$M \leq A_2 N \tag{32}$$

in the notation of (13) and consider the contribution to $T_1(n, M)$ due to those values of r, s, ρ, σ meeting its conditions of summation for which

$$\max_{1\leq i\leq \ell} \left|L_i(r,s)\right| = \left|L_u(r,s)\right| \text{ and } L_u(r,s) = m \tag{33}$$

for some specified integer m of a size between M inclusive and $2M$ exclusive. In these surroundings the requirement that $0 < f(r,s) = f(\rho,\sigma)$ implies that

$$\left|m\right| = \left(L_u(r,s), \prod_{1\leq j\leq \ell} L_j(\rho,\sigma)\right) \leq \prod_{1\leq j\leq \ell} \left(L_u(r,s), L_j(\rho,\sigma)\right)$$

so that at least one factor $(L_u(r,s), L_v(\rho,\sigma))$ on the right above is not less that

$$\left|m\right|^{1/\ell} \geq M^{1/\ell}, \tag{34}$$

the value μ of $L_v(\rho,\sigma)$ being governed by the condition $0 < \left|\mu\right| \leq \left|m\right| < 2M$ through the definition of $T_1(n)$. Hence, since $\left|s\right|,\ \left|\sigma\right| < 2A_1 M = A_6 M$ by (12), we deduce that

$$T_1(n,M) \leq \sum_{1\leq u,v\leq \ell} \sum_{\substack{0<|m|,|\mu|<2M \\ (m,\mu)\geq M^{1/\ell}}} T_{u,v}(n,M;m,\mu), \tag{35}$$

where $T_{u,v}(n,M;m,\mu$ is the number of solutions of (29) in integers s, σ of size not exceeding $A_6 M$ that do not appertain via (25) and (26) to the association $(r,s) \simeq (\rho,\sigma)$.

Let us first depose of the contribution $T_1^*(n,M)$ to the right-hand side of (35) that relates to values of u, v, m, μ for which the polynomial $mF(m,s) - \mu G(\mu,\sigma)$ is reducible. In this case, by (31), m and μ are connected by an equation $B_{u,v}m = C_{u,v}\mu$ for one of a finite set of pairs of coprime non-zero integers $B_{u,v}, C_{u,v}$. Also, the zeros of $mF(m,s) - \mu G(\mu,\sigma)$ are distributed among all its irreducible factors with rational coefficients, each such factor of degree 2 or more having $O\left(M^{\frac{1}{2}+\epsilon}\right)$ zeros in the chosen domain of s and σ by Lemma 1. On the other hand, the zeros of any linear factors are inadmissible because we have shewn earlier that they would not meet the stipulation that $(r,s) \not\simeq (\rho,\sigma)$. Consequently

$$T_1^*(n,M) = O\left(M^{\frac{3}{2}+\epsilon}\right) \tag{36}$$

by (35).

If we write

$$m = dm',\ \mu = d\mu',\ \text{where}(m',\mu') = 1 \text{ and}^3\ d \geq M^{1/\ell} \tag{37}$$

[3] When $d > 2M$ all our subsequent calculations are true but trivial, the underlying sums being of course empty.

in the conditions of summation for the remaining portion $T_1^{\dagger}(n, M)$ of the sum in the right of (35), equation (28) takes the form

$$m'F(m, s) = \mu' G(\mu, \sigma), \tag{38}$$

which with (27) and (37) implies both the congruences

$$\Phi(m, s) = \prod_{i \neq u} \left\{ h_i m + \left(h_u k_i - h_i k_u \right) s \right\} \equiv 0, \mod \mu'', \tag{39}$$

and

$$\Gamma(\mu, \sigma) = \prod_{j \neq v} \left\{ h_j \mu + \left(h_v k_j - h_j k_v \right) \sigma \right\} \equiv 0, \mod m'' \tag{40}$$

for certain coprime moduli

$$m'' = m'/a, \quad \mu'' = \mu'/\alpha$$

derived from the division of m' and μ', respectively, by certain (small) positive divisors a and α of $\left(m', h_u^{\ell-1}\right)$ and $\left(\mu', h_v^{\ell-1}\right)$. Even though $\Phi(m, s)$ and $\Gamma(\mu, \sigma)$ are products of rational linear factors, a full discussion of these congruences for general composite moduli having repeated prime factors entails the same sort of difficulties that attend the general theory of polynomial congruencies in one variable as expounded by Nagell ([4], ch. III); these difficulties at the present juncture would in fact involve the prime divisors of the discriminants of $\Phi(m, s)$ and $\Gamma(\mu, \sigma)$ quâ polynomials in s and σ and, therefore, ultimately and especially those of the number d. However, at the expense of a balancing slight lengthening in procedure, we are able here to circumvent these congruential entanglements by reducing our situation to one where the moduli are square-free.

Accordingly, for integers m'' and μ'' in (40) and (39) whose expressions in terms of prime factors are stated as

$$m'' = \pm \prod_p p^b, \quad \mu'' = \pm \prod_{\varpi} \varpi^{\beta}, \text{ say,}$$

we shall first use the *positive* square-free numbers

$$m_3 = \prod_p p, \quad \mu_3 = \prod_{\varpi} \varpi,$$

while later we shall need numbers m_4, μ_4, that similarly originate from m', μ' and bear no relation to a and α; finally, for each given number of type m_4 or μ_4, we let $m_5 = m_5(m_4)$ or $\mu_5 = \mu_5(\mu_4)$ denote positive numbers whose prime factors are divisors of m_4 and μ_4, respectively. Then, the procedure being amply illustrated by reference to the congruence (40), all solutions of this in σ satisfy the corresponding congruence taken to the modulus m_3, the number of incongruent solutions of which we denote by $\kappa(m_3)$. Since $\kappa(m_3)$ is multiplicative, it suffices to consider $\kappa(p)$ when $p \nmid D$ because in the contrary instance we are content with the trivial estimate $\kappa(p) \leq p$. Thus we may assume that the coefficient of σ in each factor of $\Gamma(\mu, \sigma)$ in (40) is indivisible by p and deduce that each such factor is divisible by p when σ belongs to just one residue class, mod p. Consequently, we see that $\kappa(p)$ does not exceed p or $\ell - 1$ according as $p|D$ or $p \nmid D$ and conclude both that

$$\kappa(m_3) = O\left\{ (\ell - 1)^{\omega(m_3)} \right\} = O\left(m_3^{\epsilon} \right) \tag{41}$$

and that a similar result holds for the other congruence (39).

In the current circumstances the solutions of (38) in s, σ have been shewn to be distributed into $O(M^{\epsilon})$ sets, each of which consists of pairs of numbers of the type

$$s = s_0 + s_1\mu_3, \quad \sigma = \sigma_0 + \sigma_1 m_3 \tag{42}$$

for certain positive numbers s_0, σ_0 not exceeding μ_3, m_3 respectively. The relevant contribution to $T_{u,v}(n, M; m, \mu)$ corresponding to each set is then obtained by substituting (42) in (38) to obtain an irreducible equation is s_1, σ_1 of degree $\ell - 1$, of which, being constrained by the inequalities

$$|s_1| \le \frac{A_6M + \mu_3}{\mu_3} < \frac{2A_6M}{\mu_3}(> 1), \ |\sigma_1| \le \frac{A_6M + m_3}{m_3} < \frac{2A_6M}{m_3}(> 1),$$

the number of qualifying pairs of zeros is

$$O\left(M^{1/(\ell-1)+\epsilon} \max\left(\frac{1}{\mu_3}, \frac{1}{m_3}\right)^{1/\ell-1}\right) = O\left(M^{1/(\ell-1)+\epsilon} \max\left(\frac{1}{\mu_4}, \frac{1}{m_4}\right)^{1/(\ell-1)}\right)$$

by Lemma 1. Therefore, taking stock after this, (41), (35), and (37), we conclude that

$$T_1^{\dagger}(n, M) = O\left(M^{1/(\ell-1)+\epsilon} \sum_{d \ge M^{1/\ell}} \sum_{0<m',\mu' \le 2M/d} \max\left(\frac{1}{m_4}, \frac{1}{\mu_4}\right)^{1/(\ell-1)}\right), \tag{43}$$

from which the estimate for $T_1^{\dagger}(n, M)$ will flow by the way of the simple

Lemma 3. *Let q denote any positive integer composed entirely of prime factors* (*possibly repeated*) *that divide a given positive number* (*possibly* 1) *not exceeding z. Then the number of q not exceeding z is $O(z^{\epsilon})$.*

This is a special case of the Lemma 4 in [3]. Evidently the inner sum in (43) does not exceed

$$\begin{aligned}
2 \sum_{0<m',\mu' \le 2M/d} \frac{1}{m_4^{1/(\ell-1)}} &= O\left(\frac{M}{d} \sum_{0<m' \le 2M/d} \frac{1}{m_4^{1/(\ell-1)}}\right) \\
&= O\left(\frac{M}{d} \sum_{0<m_4 \le 2M/d} \frac{1}{m_4^{1/(\ell-1)}} \sum_{m_5 \le 2M/m_4 d} 1\right) \\
&= O\left(\frac{M^{1+\epsilon}}{d} \sum_{0<m \le 2M/d} \frac{1}{m^{1/(\ell-1)}}\right) \\
&= O\left(\frac{M^{2-1/(\ell-1)+\epsilon}}{d^{2-1/(\ell-1)}}\right)
\end{aligned}$$

with the implication that

$$T_1^{\dagger}(n, M) = O\left(M^{2+\epsilon} \sum_{d \ge M^{1/\ell}} \frac{1}{d^{2-1/(\ell-1)}}\right) = O\left(M^{2-(\ell-2)/\ell(\ell-1)+\epsilon}\right),$$

wherefore on taking this with (36) we have

$$T_1(n, M) = O\left(M^{2-(\ell-2)/\ell(\ell-1)+\epsilon}\right) \tag{44}$$

for $M \le A_2 N$ as in (32).

Similar principles are successful for the estimation of $T_1(n, M)$ in the complementary range $A_2 N < M < A_4 n^{1/(\ell-1)}$ but are less straightforward to apply. Now, by the definition of $T_1(n, M)$ and (16), we first modify (33) by using the (unique) subscript u for which $L_u(r, s)$ equals a non-zero number m whose size does not exceed

$$M_I = A_5 n / M^{\ell-1} < M, \tag{45}$$

even though the previously used inequalities for s, σ are still valid. Next, following previous thinking, we find there is a subscript v for which the number $\mu = L_v(\rho, \sigma)$ possesses the properties

$$(m, \mu) \ge |m|^{1/\ell} \quad \text{and} \quad |\mu| < 2M. \tag{46}$$

This clears the way for a reconsideration of $T_1^{\dagger}(n, M)$ because the assessment

$$T_1^*(n, M) = O\left(M^{\frac{1}{2}+\epsilon} M_I\right) \tag{47}$$

is a corollary of (31).

The new surroundings affect the sums bounding $T_1^{\dagger}(n, M)$ more in regard to the conditions of summation than the summands therein. In the former we still have the first parts of (37) but replace the last part by $d \ge |m|^{1/\ell}$ with the result that

$$0 < m' \le M_I/d, \quad 0 < m' \le d^{\ell-1}, \quad 0 < \mu' < 2M/d.$$

Hence, emulating the derivation of (43), we have

$$\begin{aligned} T_1^{\dagger}(n, M) &= O\left(M^{1/(\ell-1)+\epsilon} \sum_d \sum_{\substack{0<m' \le M_I/d, d^{\ell-1} \\ 0<\mu' \le 2M/d}} \max\left(\frac{1}{m_4}, \frac{1}{\mu_4}\right)^{1/(\ell-1)}\right) \\ &= O\left(M^{1/(\ell-1)+\epsilon} \sum_d \sum\nolimits_d\right), \text{ say,} \end{aligned} \tag{48}$$

and then go on to treat $\sum_d$ for the two cases $d > M_I^{1/\ell}$ and $d \le M_I^{1/\ell}$. In the earlier instance, by Lemma 3 and then (45), we get

$$\begin{aligned} \sum\nolimits_d &\le \sum_{\substack{0<m' \le M_I/d \\ 0<\mu' \le 2M/d}} \frac{1}{m_4^{1/(\ell-1)}} + \sum_{\substack{0<m' \le M_I/d \\ 0<\mu' \le 2M/d}} \frac{1}{\mu_4^{1/(\ell-1)}} \\ &\le \frac{2M}{d} \sum_{m_4 \le M_I/d} \frac{1}{m_4^{1/(\ell-1)}} \sum_{m_5 \le M_I/dm_4} 1 \\ &\quad + \frac{2M_I}{d} \sum_{\mu_4 \le 2M/d} \frac{1}{\mu_4^{1/(\ell-1)}} \sum_{\mu_5 \le 2M/d\mu_4} 1 \end{aligned}$$

$$= O\left(\frac{M^{1+\epsilon}}{d}\sum_{0<m\le M_I/d}\frac{1}{m^{1/(\ell-1)}}\right) + O\left(\frac{M_I M^{\epsilon}}{d}\sum_{0<\mu\le 2M/d}\frac{1}{\mu^{1/(\ell-1)}}\right)$$

$$= O\left(\frac{M^{1+\epsilon}M_I^{1-1/(\ell-1)}}{d^{2-1/(\ell-1)}}\right) + O\left(\frac{M_I M^{1-1/(\ell-1)+\epsilon}}{d^{2-1/(\ell-1)}}\right) = O\left(\frac{M^{1+\epsilon}M_I^{1-1/(\ell-1)}}{d^{2-1/(\ell-1)}}\right)$$

and in the latter instance similarly obtain

$$\sum\nolimits_d = O\left(M^{1+\epsilon}d^{\ell-3}\right)$$

after replacing M_I/d by $d^{\ell-3}$ as a limit for μ' in the summation. Therefore equation (48) can be developed into

$$T_1^{\dagger}(n, M) = O\left(M^{\ell/(\ell-1)+\epsilon}\sum_{d\le M_I^{1/\ell}} d^{\ell-3}\right)$$

$$+ O\left(M^{\ell/(\ell-1)+\epsilon}M_I^{(\ell-2)/(\ell-1)}\sum_{d>M_I^{1/\ell}}\frac{1}{d^{2-1/(\ell-1)}}\right)$$

$$= O\left(M^{\ell/(\ell-1)+\epsilon}M_I^{(\ell-2)/\ell}\right), \tag{49}$$

which in combination with (47) furnishes us with the estimate

$$T_1(n, M) = O\left(M^{\ell/(\ell-1)+\epsilon}M_I^{(\ell-2)/\ell}\right) = O\left(n^{(\ell-2)/\ell+\epsilon}M^{1-(\ell-1)(\ell-2)/\ell+1/(\ell-1)}\right) \tag{50}$$

that is the complement of (44) for the range $A_2N < M < A_4n^{1/(\ell-1)}$.

The first part of our initial theorem follows at once because the exponent of M in (50) is negative when $\ell > 3$. Indeed, by embodying (44) and (50) in (20) and then recalling (10), we deduce at once that

$$T(n) = O\left(N^{2-(\ell-2)/\ell(\ell-1)+\epsilon}\right) + O\left(n^{(\ell-2)/\ell+\epsilon}N^{1-(\ell-1)(\ell-2)/\ell+1/(\ell-1)}\right)$$

$$= O\left(N^{2-(\ell-2)/\ell(\ell-1)+\epsilon}\right)$$

or

$$T(n) = O\left(n^{2/\ell-(\ell-2)/\ell^2(\ell-1)+\epsilon}\right) \tag{51}$$

and so estimate $\nu(n)$ because of (19).

When $\ell = 3$ it is only the last part of the analysis leading to (50) that fails to be effective. Yet, if we take the opportunity that arises here to use Lemma 2 instead of Lemma 1, we can not only produce a workable alternative to (50) but find all the relevant revised estimates in the work combine to yield the board

$$T(n) = O\left(N^{2-\frac{1}{3}+\epsilon}\right) = O\left(n^{\frac{2}{3}-\frac{1}{9}+\epsilon}\right) \tag{52}$$

that is better than what would be got by formally putting $\ell = 3$ in (51). Moreover, although the general structure of the previous method is retained, there is the important simplification that all references to the congruences (39) and (40) and to Lemma 3 are avoided.

To indicate briefly what is to be done, we note that revisions are only needed when the polynomial $m'F(m,s)-\mu'G(\mu,\sigma)$ in s,σ is irreducible and hence when it has $O(M^{\epsilon})$ zeros of size not exceeding $2A_1M$ by Lemma 2. Hence we can improve (43) to

$$T_1^{\dagger}(n,M)=O\left(M^{\epsilon}\sum_{d\geq M^{1/\ell}}\ \sum_{0<m',\mu'\leq 2M/d}1\right)$$

and thus (44) to

$$T_1^{\dagger}(n,M)=O\left(M^{2-1/\ell+\epsilon}\right).$$

Similarly (48) is replaced by

$$T_1^{\dagger}(n,M)=O\left(M^{\epsilon}\sum_{d}\ \sum_{\substack{0<m'\leq M_I/d,d^{\ell-1}\\ 0<\mu'\leq 2M/d}}1\right),$$

which leads to the counterpart

$$T_1^{\dagger}(n,M)=O\left(n^{(\ell-1)/\ell+\epsilon}M^{1-(\ell-1)^2/\ell}\right)$$

of (49). The exponent of M in this being $-\frac{1}{3}$, we then sum over M as before to obtain (52) in place of (51) for $\ell=3$ and thus complete the proof of

Theorem 1. *Let $f(x,y)$ be a totally reducible binary form of degree ℓ with integral coefficients and non-zero discriminant. Then, if $\nu(n)$ be the number of positive integers up to a large number n that have essentially more than one representation by f, we have*

$$\nu(n)=O\left(n^{2/\ell-\eta_\ell+\epsilon}\right),$$

where

$$\eta_\ell=\begin{cases}1/\ell^2,\ if\ \ell=3,\\ (\ell-2)/\ell^2(\ell-1),\ if\ \ell>3.\end{cases}$$

6. The second theorem

To shew it is exceptional for a number to be represented by $f(x,y)$ in essentially more than one way we must foreshadow a simple aspect of our following paper by defining $r(m)$ to be the number of ways of expressing the positive number m by $f(x,y)$, where of course

$$r(m)=O\left\{d_\ell(m)\right\}=O\left(m^{\epsilon}\right). \tag{53}$$

Let us now take one of the semi-infinite triangular regions described in §3 in which $f(x,y)$ is positive and consider points (x,y) within having integral coordinates for which $|x|,|y|<A_8n^{1/\ell}$ for a suitably small positive constant A_8. Then $0<f(x,y)<n$ for all these points, the cardinality of which exceeds $A_9n^{2/\ell}$ by a standard lattice point argument. Consequently

$$\sum_{0<m\leq n}r(m)>\ A_8n^{2/\ell}$$

and thus, by (53),

$$\Upsilon(n) > A(\epsilon)n^{-\epsilon} \sum_{m \le n} r(m) > A(\epsilon)n^{2/\ell-\epsilon},$$

whence, on comparing this with Theorem 1, we gain the following.

Theorem 2. *Almost all the positive numbers represented by the form* $f(x, y)$ *in Theorem* 1 *are represented thus in essentially only one way*.

References

[1] Bombieri E and Pila J, The number of integral points on arcs and ovals, *Duke Math. J.* **59** (1989) 337–357
[2] Hooley C, On the representation of a number as the sum of a square and a product, *Math. Zeitschr.* **69** (1958) 211–227
[3] Hooley C, On binary cubic forms: II, *J. Reine Angew. Math.* **521** (2000) 185–240
[4] Nagell T, Introduction to Number Theory (Stockholm: Almquist and Wiksell) (1951)