Canad. Math. Bull. Vol. **28** (3), 1985

THE VALUE DISTRIBUTION OF REDUCIBLE CUBICS

BY

P. D. T. A. ELLIOTT

In memory of R. A. Smith

ABSTRACT. The representation of integers by the products and quotients of the values of $x(x^2 + a)$ at integer points is considered.

1. Let $r_1, r_2, \ldots$ be a sequence of positive rational numbers. Considering the set of all positive rationals Q^* as a group under multiplication, let Γ be its subgroup generated by the r_i, and let G be the quotient group Q^*/Γ. The group G reflects to what extent an arbitrary positive integer n has a multiplicative representation

$$n = \prod_{i=1}^{t} r_{j_i}^{\epsilon_i},$$

where every ϵ_i has the value $+1$ or -1. In particular G is trivial if and only if every integer n is so representable.

Let $F(x)$ be a rational function of x with integer coefficients, which is positive for all large positive real values of x. For any given positive integer k let $r_1, r_2, \ldots$ be the sequence of positive rationals amongst the $F(m)$ when m runs through the positive integers exceeding k. I conjecture that for all large k the group G is independent of k, and that for squarefree $F(x)$ it is the direct sum of a free group and a finite group.

As an example, G is free when $F(x) = x^2 + 1$. Evidence for the conjecture is marshalled in my book [3]. As I there indicate, little is known when $F(x)$ involves terms of degree 3 or higher. In the present paper I investigate the cases $F(x) = x(x^2 + a)$ for non-zero integers a.

For the remainder of the paper $w(x)$ will be a reducible cubic $x(x^2 + a)$ where $-a$ is an integer which is not a square. Unless otherwise indicated the rational functions which appear in the arguments have integer coefficients, although it will be seen that these arguments can be largely carried out in an arbitrary commutative ring which has an identity but no divisors of zero.

When $-a$ is a non-zero square, the result of my paper [2] shows that G is trivial.

Surprisingly the cubics $w(x)$ satisfy a multiplicative identity.

THEOREM 1. *There are polynomials $H_i(x)$, $i = 1, \ldots, t$, of degree at most 4, and integers $\epsilon_i = \pm 1$, so that*

Received by the editors May 15, 1984 and, in revised form December 13, 1984.
AMS Subject Classification: 10H99, 10K20, 10M05.

$$x^6 = \prod_{i=1}^{t} w(H_i(x))^{\epsilon_i}$$

in the field of rational functions of x over Q.

The polynomials $H_i(x)$ may be readily computed. As I presently show, only two of them need to be of degree 4, the rest may be quadratic or linear. In particular every polynomial has a positive leading coefficient. Thus every element of the above group G has in this case an order of at most 6. This can be improved.

THEOREM 2. *Every positive integer m has a representation of the form*

$$m^2 = \prod_{j=1}^{s} w(n_j)^{\epsilon_j}$$

where each positive integer n_j has at most a polynomial growth in m, and $\epsilon_j = \pm 1$. If the restriction on the size of the n_j is omitted, there are infinitely many representations.

For $F(x) = x(x^2 + a)$ the group G is either trivial, or an infinite direct product of groups of order 2.

As an application of Theorem 1 I prove

THEOREM 3. *Let $\delta = 144(a + 1)^3(a + 2)$. Then every positive integer m has infinitely many representations of the form*

$$m^{\delta} = \prod_{j=1}^{t} \left(\frac{w(n_j)w(n_j + 2)}{w(n_j + 1)^2} \right)^{\epsilon_j}$$

with n_j a positive integer, $\epsilon_j = \pm 1$.

The value of δ in this theorem can be improved at once to $48(a + 1)^3$, perhaps further, but since Theorem 3 serves only as an illustration I do not pursue this matter.

2. LEMMA 1. *Let $Q(t) = \alpha t^2 + \beta t + \gamma$, $\alpha \neq 0$, be a polynomial with rational coefficients. Let M be a non-zero rational number. Then*

$$Q(M^{-1}Q(t) + t) = M^{-2}\alpha Q(t)Q(t + M\alpha^{-1}).$$

PROOF. This can be verified directly.

Consider now the reducible cubic $z(t) = t(t^2 + bt + c)$ where b, c are integers, not both zero. We apply Lemma 1 with $Q = t^2 + bt + c$ to obtain

$$\frac{z(M^{-1}Q + t)}{z(t)z(t + M)} = \frac{M^{-3}(Q + Mt)}{t(t + M)}. \tag{1}$$

Here progress will be made if we can choose M to be an integer so that $Q + Mt$ is reducible over $\mathbb{Z}[t]$. This needs $(M + b)^2 - 4c = r^2$ for some integer r. This is always possible, for example with $M + b = c + 1$, $r = c - 1$. With these choices for M and r, $Q(t)$ will be divisible by M in $\mathbb{Z}$ provided t is specialized to satisfy $t + 1 \equiv 0 \pmod{M}$ or $t + b - 1 \equiv 0 \pmod{M}$.

If we set $t = (c + 1 - b)y - 1$, then with certain integers a_j the left-hand side of

(1) has the alternative representation

$$M^{-3}\left(\frac{My + a_1}{My - 1}\right)\left(\frac{My + a_2}{M[y + 1] - 1}\right) = S(y),$$

say. One would expect that every positive integer g had a representation

$$g = \prod_{i=1}^{k} S(n_i)^{\epsilon_i}, \quad \epsilon_i = \pm 1,$$

perhaps with $n_i < c(\theta)g^{1+\theta}$ for each fixed $\theta > 0$. This would establish the conjecture for $F(x) = x(x^2 + bx + c)$. However, at the moment this line of argument seems difficult to follow.

Instead I take $b = 0$, $c = a$ and restrict myself to $w(x)$.

LEMMA 2. *If $x = (a + 1)y$ then in the ring $Z[y]$ there are polynomials $F_i(y)$ of degree at most 4 so that*

$$\frac{x^3(x^2 + a - 1)}{x^2 - 1} = \prod_{i=1}^{s_1} w(F_i(y))^{\epsilon_i}, \qquad \epsilon_i = \pm 1.$$

PROOF. With $Q = t^2 + a$, $M = a + 1$ the identity (1) becomes

$$\frac{w\left(\frac{t^2 + a}{1 + a} + t\right)w(1)^3}{w(t)w(t + 1 + a)} = \frac{(t + 1)(t + a)}{t(t + 1 + a)} \tag{2}$$

This will be useful so long as we specialize t so that $(t^2 + a)/(1 + a)$ can be interpreted as a polynomial with integer coefficients.

Replacing t by $x^2 - 1$ where $x = (a + 1)y$ now gives the desired relation, since $x^2 + a = w(x)x^{-1}$.

3. For polynomials P_1, P_2 in $\mathbb{Z}[x]$ we write $P_1 \sim P_2$ if in the field of rational functions of x (with integer coefficients) there is an identity

$$P_1P_2^{-1} = \prod_{i=1}^{\ell} w(G_i(x))^{\epsilon_i}$$

with $G_i(x)$ in $\mathbb{Z}[x]$ and $\epsilon_i = \pm 1$. This is an equivalence relation.

Group theoretically, let θ be the multiplicative group of rational functions of x with integer coefficients, and let Γ_1 be the subgroup generated by the $w(G(x))$ where $G(x)$ belongs to $\mathbb{Z}[x]$. Then $P_1 \sim P_2$ if and only if P_1 and P_2 belong to the same coset mod Γ_1. As for G, we aim to determine the group θ/Γ_1.

In the following arguments Lemma 1 with $M = 1$ will be applied many times.

LEMMA 3.

$$x^2 + a - 1 \sim (x - 1)x^3(x + 1)$$

PROOF. By definition the polynomial $h_1 = h_1(x) = x^2 + a$ satisfies $h_1 \sim x^{-1}$.

https://doi.org/10.4153/CMB-1985-039-8 Published online by Cambridge University Press

Replacing x by $h_1 + x$ and appealing to Lemma 1

$$(h_1 + x)^{-1} \sim h_1(h_1 + x) = h_1(x)h_1(x + 1) \sim x^{-1}(x + 1)^{-1},$$

which gives

$$h_2 = h_2(x) = x^2 + x + a \sim x(x + 1).$$

We now replace x in this identity by $h_2 + x$.

$$(h_2 + x)(h_2 + x + 1) \sim h_2(h_2 + x) = h_2(x)h_2(x + 1)$$
$$\sim x(x + 1)(x + 1)(x + 2).$$

Here

$$h_2 + x + 1 = x^2 + 2x + a + 1 = (x + 1)^2 + a \sim (x + 1)^{-1}$$

giving

$$x^2 + 2x + a \sim x(x + 1)^3(x + 2)$$

Replacing x by $x - 1$ the lemma is established.

PROOF OF THEOREM 1. From Lemma 2 and Lemma 3 we obtain an identity

$$((a + 1)y)^6 = \prod_{i=1}^{s_2} w(H_i(y))^{\epsilon_i},$$

and note that $a + 1 = w(1)$.

4. Let us say that a rational function $R(x)$ in $\mathbb{Z}(x)$ has *persistence of form* if there are distinct non-constant polynomials $T_i(x)$ in $\mathbb{Z}[x]$ and integers d_i, positive, negative but not all zero, such that

$$\prod_{i=1}^{j} R(T_i(x))^{d_i} = \text{constant}.$$

From Theorem 1, using x and $2x$, we see that $x(x^2 + a)$ has persistence of form. Persistence of form is useful in establishing product representations, as I shall illustrate in the proof of Theorem 3.

In fact in the representation of x^6 in Theorem 1 one may take

$$H_1(x) = \frac{(z^2 - 1)^2 + a}{1 + a} + z - 1, \qquad \epsilon_1 = 1,$$

$$H_2(x) = h_1(h_2(z - 1) + z - 1) + h_2(z - 1) + z - 1, \qquad \epsilon_2 = 1.$$

with $z = (a + 1)x$, and degree $H_i \leq 2$ for all $i \geq 3$.

5. Let us now write $A \approx B$ if the polynomials A, B in $\mathbb{Z}[x]$ satisfy

$$AB^{-1} = u^3 \prod_i w(J_i)^{\epsilon_i}$$

https://doi.org/10.4153/CMB-1985-039-8 Published online by Cambridge University Press

with polynomials J_i in $\mathbb{Z}[x]$ and a rational function u with integer coefficients. We are thus working mod. the group $(\theta/\Gamma_1)^3$. In particular $A \sim B$ implies $A \approx B$.

Consider the polynomial $s = s(x) = x^2 + a - 1$. From Lemma 3, since cubes now become units, $s(x) \approx x^2 - 1$. Replacing x by $s + x$ in this last relation we have on the one hand

$$\begin{aligned} s(s + x) &\approx (x^2 + x + a)(x^2 + x + a - 2) \\ &\approx x(x + 1)(x^2 + x + a - 2) \end{aligned}$$

since $h_2 \sim x(x + 1)$. On the other hand, another application of Lemma 1 gives

$$s(s + x) = s(x)s(x + 1) \approx (x^2 - 1)([x + 1]^2 - 1).$$

Altogether therefore

$$x^2 + x + a - 2 \approx (x - 1)(x + 2).$$

Writing $s_1(=s_1(x))$ for the polynomial involving $a - 2$ we continue this process.

$$\begin{aligned} s_1(s_1 + x) &\approx (s_1 + x - 1)(s_1 + x + 2) \\ &\approx (x^2 + 2x + a - 3)(x^2 + 2x + a) \\ &\approx (x^2 + 2x + a - 3)x(x + 2) \end{aligned}$$

since

$$x^2 + 2x + a = (x + 1)^2 + a - 1 \approx ([x + 1]^2 - 1).$$

Moreover, by Lemma 1

$$s_1(s_1 + x) = s_1(x)s_1(x + 1) \approx (x - 1)(x + 2)x(x + 3).$$

These relations combine to give

$$x^2 + 2x + a - 3 \approx (x - 1)(x + 3).$$

Replacing x by $x - 1$ we arrive at

$$x^2 + a - 4 \approx (x - 2)(x + 2)$$

Comparing this relation with the initial

$$x^2 + a - 1 \approx (x - 1)(x + 1)$$

the optimistic might hope that this process continues forever; unbelievably, it does!

LEMMA 4. *For each positive integer m*

$$\begin{aligned} x^2 + x + a - m^2 + m &\approx (x - m + 1)(x + m) \\ x^2 + a - m^2 &\approx (x - m)(x + m) \end{aligned}$$

PROOF. Using the pair of relations there is no difficulty in establishing this result by induction on m.

https://doi.org/10.4153/CMB-1985-039-8 Published online by Cambridge University Press

LEMMA 5. *There are integers* b_j, $j = 1, \ldots, 4$, *for which the relation*

$$\frac{(x - b_1)(x - b_2)}{(x - b_3)(x - b_4)} \approx 1$$

holds nontrivially.

PROOF. If a is odd or 4 divides a, then we can write it in the form $r^2 - s^2$ using either $r = (a + 1)/2$, $s = (a - 1)/2$; or $r = (a + 4)/4$, $s = (a - 4)/4$, respectively. From the second relation of Lemma 4, with $m = r$, we obtain

$$\frac{(x - s)(x + s)}{(x - r)(x + r)} \approx 1,$$

since then $x^2 + a - m^2 = x^2 - s^2$ and is reducible. This relation is trivial only if $r = -s$ or equivalently $a = 0$, a case ruled out earlier.

If a is even, but only divisible by 2, then it can be expressed in the form $a = (c - k)(c + k - 1)$. One such representation is given by $a = a_1 a_2$, $c = (a_1 + a_2 + 1)/2$, $k = (a_2 - a_1 + 1)/2$ provided that a_1 and a_2 have different parity. Then $4a = (2c - 1)^2 - (2k - 1)^2$ and the quadratic polynomial $x^2 + x + a - c^2 + c$ is reducible, since its discriminant is $(2k - 1)^2$. With $a_1 = a/2$, $a_2 = 2$, $c = (a + 6)/4$, $k = -(a - 6)/4$ we obtain from the first relation of Lemma 4

$$\frac{(x + k)(x - k + 1)}{(x + c)(x - c + 1)} \approx 1.$$

This will be non-trivial unless $c = k$ or $c = -k + 1$, possibilities which also correspond to $a = 0$.

Lemma 5 is established.

The result of this lemma allows us to assert, bearing in mind the underlying cubes and applying Theorem 1, that

$$\left(\frac{(x - b_1)(x - b_2)}{(x - b_3)(x - b_4)}\right)^2 = \prod_{i=1}^{s_3} w(K_i(x))^{\epsilon_i}, \qquad \epsilon_i = \pm 1 \tag{3}$$

for appropriately chosen polynomials $K_i(x)$ in $\mathbb{Z}[x]$. Note that in this identity the degrees of the polynomials $K_i(x)$ increase exponentially with $|a|$. Perhaps such an identity exists with exponent 1 in place of the 2, but working mod. the group $(\theta/\Gamma_1)^2$ which is presently called for doesn't seem to lead to great simplification.

PROOF OF THEOREM 2. Let $R(x)$ be a rational function of the form

$$\prod_{i=1}^{t} (x - b_i)^{d_i}$$

where the b_i are distinct integers, and the integers d_i have highest common factor 1. I proved [1] that every positive integer m has a representation

$$m = \prod_{j=1}^{h} R(n_j)^{\epsilon_j}$$

where the positive integers n_j do not exceed cm for some constant c depending only upon $R(x)$. This together with (3) establishes a representation of the type asserted in Theorem 2.

The second assertion is similarly obtained.

6. Consider now the rational function

$$L(t) = \frac{w(t)w(t+2)}{w(t+1)^2} = \frac{t(t+2)(t^2+a)(t^2+4t+a+4)}{(t+1)^2(t^2+2t+a+1)^2}.$$

Let $f: Q^* \to \mathbb{R}/\mathbb{Z}$ be an additive arithmetic function with values (mod 1) which satisfies $f(L(n)) = 0$ for all sufficiently large integers n, say $n > n_0$. Thus if Γ is the subgroup of Q^* generated by the (assumed positive) $L(n)$ with $n > n_0$, then f is a homomorphism of the group Q^*/Γ into the (additive) group $\mathbb{R}/\mathbb{Z}$.

In terms of the shift operator E which takes the sequence $(v_1, v_2, \dots)$ to the sequence $(v_2, v_3, \dots)$ we have

$$(E-1)^2 f(w(n)) = 0 \text{ for } n > n_0.$$

This is a linear recurrence which may be solved to give

$$f(w(n)) = \lambda n + \mu, \qquad n > n_0. \tag{4}$$

for some constants λ, μ.

We now employ the persistence of form of $w(t)$. From Theorem 1

$$x^6 = w(H_1(x))w(H_2(x)) \dots$$

This holds also if we replace x by kx, so by division

$$w(H_1(kx))w(H_2(kx))w(H_1(x))^{-1}w(H_2(x))^{-1} \prod_{i=1}^{s_4} w(N_i)^{\epsilon_i} = k^6 \tag{5}$$

where the N_i are quadratic polynomials in $\mathbb{Z}[x]$, possibly depending upon k, but s_4 is an integer not depending upon k.

Combining this last relation with (4) we see that

$$\lambda[H_1(kx) + H_2(kx) - H_1(x) - H_2(x)] + (\text{terms of degree} \leq 2 \text{ in } x) = 0$$

provided $k \geq 1$ is fixed, and x is a positive integer exceeding n_0. This in turn gives

$$\lambda[(a+1)^3(k^4-1)x^4 + (a+1)^4(k^4-1)x^4] + (\text{terms of lower degree in } x) = 0 \tag{6}$$

We now appeal to

LEMMA 6. *If a polynomial $\phi(x)$, of degree r, with coefficients in $\mathbb{R}/\mathbb{Z}$, satisfies $\phi(n) = 0$ for all sufficiently large positive integers n, then $r!\phi(x)$ is identically zero.*

PROOF. A proof by induction on the degree r is readily constructed. The polynomial

$$\frac{1}{r!}\prod_{j=0}^{r-1}(x-j)$$

shows that the coefficient $r!$ in the conclusion cannot in general be decreased.

In view of this lemma our relation (6) yields $4!\lambda(a+1)^3(a+2)(k^4-1) \equiv 0 \pmod 1$. Since 2^4-1 (=7) and 3^4-1 (=80) are coprime, there are integers α, β so that $\alpha(2^4-1)+\beta(3^4-1)=1$. Therefore, choosing $k=2,3$ in turn we deduce that $4!\lambda(a+1)^3(a+2) \equiv 0 \pmod 1$. Hence

$$4!(a+1)^3(a+2)f(w(n)) = \mu$$

a constant, holds for all $n > n_0$.

Returning now to the relation (5) and applying f:

$$\mu \sum_{i=1}^{s_4} \epsilon_i = 4(a+1)^3(a+2)6f(k)$$

and since s_4 is independent of k,

$$4!(a+1)^3(a+2)6f(k) = \text{constant}$$

This holds for all positive k, including $k=1$, which shows that the constant is zero.

We have now proved that every homomorphism f: $Q^*/\Gamma \to \mathbb{R}/\mathbb{Z}$ is trivial on the δ^{th} powers of integers, where $\delta = 4!(a+1)(a+2)6$. Hence as in Lemma 5 of my paper [2] in the Journal of the Australian Mathematical Society, there is a representation of the type asserted in the statement of Theorem 3.

This proves Theorem 3. In fact, employing the earlier identity (3) involving the polynomials K_i, the exponent δ can be reduced to $4!(a+1)^3(a+2)2$. Perhaps an even smaller exponent may be obtained by pursuing the particular form of the polynomials K_i and H_j.

7. The only accessible results on the value distribution of reducible cubics seem to be those of Burgess [1], the short note of his contribution to the meeting in honor of I. M. Vinogradov's eightieth birthday. There Burgess considers the polynomials $g(x) = x(x^2 - c(c+1))$ in particular, and gives the identity (2). His interest lay in the consideration of $\chi(g(x))$ for Dirichlet characters χ.

I became interested in examples of the group G and remembered Burgess' paper, Lemma 1 represents my attempt to give a rationale for his identity (2). Lately, I wrote to him to enquire of his further researches and found to my surprise that his methods, which apply to the value distribution of polynomials at both positive and negative integers, have a different basis, and therefore lead to results different from those presented here. Note that if one allows both positive and negative integers, then the rôle of the group G will be played by $G_1 = Q_1^*/\Gamma_2$ where Q_1^* is the multiplicative group of non-zero rationals and Γ_2 is its subgroup generated by the values of $R(x)$ and $R(-x)$ with positive integer specialisations of x. Almost certainly the assertion of the general conjecture concerning G can be made concerning the group G_1.

REFERENCES

1. D. A. Burgess, *Dirichlet Characters and Polynomials*, Proc. International Conf. on Number Theory, Moscow, 14–18 Sept., 1971. Trud. Mat. Inst. Steklov, CXXXII, Moscow, 1973.

2. P. D. T. A. Elliott, *On representing integers as products of integers of a prescribed type*, J. Australian Math. Soc. (Series A) **35** (1983), pp. 143–161.

3. ———*Arithmetic Functions and Integer Products*, Grundlehren der math. Wiss. 272 Springer Verlag N.Y. 1985.

DEPARTMENT OF MATHEMATICS
BOX 426, UNIVERSITY OF COLORADO,
BOULDER, COLORADO 80309, U.S.A.