TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 299, Number 1, January 1987

PERSISTENCE OF FORM AND THE VALUE GROUP OF REDUCIBLE CUBICS

P. D. T. A. ELLIOTT

ABSTRACT. It is proved that the values of $x(x^2 + c)$, $c \neq 0$, at positive integers, multiplicatively generate the positive rationals. Analogs in rational function fields are obtained.

1. Let Q^* be the multiplicative group of positive rational numbers. Let r_1, $r_2, \ldots$, be a sequence of positive rationals, and Γ the subgroup of Q^* which they generate. Let G be the quotient group Q^*/Γ. This group G reflects the extent to which an arbitrary positive integer has a multiplicative representation by the r_n. Since Q^* is freely generated by the positive prime numbers, G models an arbitrary denumerable abelian group, and an algorithm to determine its structure cannot be given. However, this situation could change if the r_n were given enough algebraic properties.

Let $F(x)$ be a rational function P_1/P_2, the P_i in $Z[x]$ and having positive leading coefficients. Let θ be a nonnegative real number, and choose for the sequence of rationals r_n the positive values among the $F(t)$ as t runs through the integers greater than θ. In my book [**4**] and paper [**5**] I made early versions of the following conjectures:

(i) For all sufficiently large θ, G *is independent of* θ.

(ii) If F is an irreducible polynomial, or more generally a squarefree rational function, then G *is the direct sum of a free group and a finite group.*

A consequence of these conjectures would be that those positive integers m which have representations of the form

$$m^k = \prod_{i=1}^{d} F(t_i)^{\varepsilon_i}, \qquad \varepsilon_i = \pm 1,$$

with positive integers t_i, would possess infinitely many of them. Moreover the same fixed value of k could be taken for all m. To some extent this is a multiplicative analogue of Waring's problem (cf. Vaughan [**8**]).

In an abuse of notation I shall write $Q^*/\Gamma(F(n))$ for G, notationally suppressing the possible dependence on θ.

I have verified these conjectures for the following classes of functions.

A. $F(x) = x^2 + bx + c$ for integers b, c with $b^2 \neq 4c$. Thus when $F(x) = x^2 + 1$, the group G is free with generators the $p \pmod{\Gamma}$ for primes $p \equiv 3 \pmod 4$.

B. $F(x) = \prod_{j=1}^{k}(x - a_j)^{b_j}$ with distinct integers a_j, and integers b_j which have highest common factor 1. In this case G is trivial.

Received by the editors December 12, 1985.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 10H99, 10K20, 10M05.
Partially supported by NSF contract DMS-8500949.

In addition, I have verified conjecture (ii) when

C. $F(x) = (ax+b)/(cx+d)$ where $a > 0$, $c > 0$, b, d are integers for which $ad \neq bc$. The free group then has finite rank, and the finite group can have arbitrarily large order.

Case B was established in [**6**]. A second presentation of the argument along with the (considerably complicated) consideration of C I included in my book [**4**]. I shall sketch a proof of case A below.

In this paper I consider the cases $F(x) = w(x) = x^k(bx^2 + a)^l$ where a and k are nonzero integers, b, l are positive integers. In particular I establish

THEOREM 1. *Both conjectures are valid if $F(x)$ has the form $x^{-1}(bx^2 + a)$ or $x(x^2 + a)$ for integers $a \neq 0$, $b > 0$.*

2. Let $Q(x)^*$ be the multiplicative group generated by the rational functions P_1/P_2 in the previous section. For a given rational function $S(x)$ in $Q(x)^*$ let $\Delta(S(x))$ be the subgroup of $Q(x)^*$ which is generated by the $S(K(x))$ where $K(x)$ is a polynomial in $Z[x]$ with positive leading coefficient. Define the quotient group $H(S(x)) = Q(x)^*/\Delta(S(x))$.

One might hope to determine the group $Q^*/\Gamma(F(n))$ by investigating its polynomial analogue $H(F(x))$, and in this way obtain parametrized product representations. In fact I shall establish

THEOREM 2. *The group $H(x^{-1}(bx^2 + a))$ with $a \neq 0$, $b > 0$ is trivial, but $H(x(x^2 + a))$ is cyclic of order 3, generated by the image of x.*

Following the proofs of these theorems I discuss related results, and give applications to the study of Dirichlet character values.

3. We say that a rational function $F(x)$ has *persistence of form* if there are distinct polynomials $K_i(x)$ in $Z[x]$, with positive leading coefficients, and integers d_i not all zero, so that

$$\prod_{i=1}^{r} F(K_i(x))^{d_i} = \text{constant}$$

holds identically. It is not clear which rational functions have persistence of form, nor how many such relations can exist for a given function $F(x)$. Some pause is induced by noting that the composition of two irreducible polynomials can be reducible. If $f(x)$ is in $Z[x]$, then Taylor's theorem shows that $f(f(x) + x)$ is divisible by $f(x)$ in $Z[x]$, and an example is furnished by $f(x) = x^2 + 1$.

In this section I consider the persistence of form of quadratic polynomials.

LEMMA 1. *Let $h(t) = \alpha t^2 + \beta t + \gamma$, $\alpha \neq 0$. Then*

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

PROOF. This identity, considered to hold between rational functions of t, α, β, γ and M, can be verified directly.

As an example in the application of Lemma 1, I establish the conjectures for the irreducible quadratic polynomials $h(x)$ of the form $x^2 + bx + c$, $c \neq 0$.

Let ϕ denote the canonical map $Q^* \to Q^*/\Gamma(n^2 + bn + c)$, for some fixed underlying $\theta > |c|$. Let $\bar{r}$ denote the image of a rational number r under this map.

Let s be the product of the $h(r)$ with integers r, $|r| \leq b + \theta$. Let q be a prime, not dividing s, for which the Legendre symbol satisfies $((b^2 - 4c)/q) = 0$ or 1. The polynomial $x^2 + bx + c$ splits (mod q), say as $(x - u)(x - v)$ where u, v can be represented by integers in the interval $[\theta + |b| + 1,\ q - |b| - 1]$. Since $u + v \equiv -b \pmod{q}$ and $0 < u + v + b < 2q$, we have $u + v = q - b$. Without loss of generality we shall assume that $0 < u < (q + |b|)/2$.

Under the map ϕ we obtain $\bar{q} = \phi(q^{-1}h(u))$ where $0 < q^{-1}h(u) < q$ for all large enough q. The subgroup G_1 of G which is generated by these $\bar{q}$ is thus finitely generated.

Moreover, applying Lemma 1 with $\alpha = 1$, $M = q$, $t = u$ we obtain $\bar{q}^2 = \bar{1}$. Thus G_1 is finite, of order k say.

Consider now a relation

$$\prod_{i=1}^{I} \bar{p}_i^{\lambda_i} \prod_{j=1}^{J} \bar{q}_j^{\mu_j} = \bar{1}$$

with integers λ_i, μ_j, primes p_i for which $((b^2 - 4c)/p_i) = -1$, and primes q_j for which this symbol has value 0 or 1. Raising everything to the kth power gives

$$\phi\left(\prod_{i=1}^{I} p_i^{\lambda_i k}\right) = \bar{1}.$$

A relation of this kind is possible only if each p_i divides $n_i^2 + bn_i + c$ for some integer n_i, and this the condition on the Legendre symbol rules out. Thus every $\lambda_i = 0$.

It is clear that G is the direct sum of a free group and of G_1. The finite G_1 has order which is a power of 2.

Suppose now that $Q(m) > 0$ for all integers $m > z$. Since

$$Q(m) = Q(Q(m) + m)/Q(m + 1)$$

we see that if the ratio of two rationals has a product representation in terms of $Q(n_i)$ with integers $n_i \geq \theta > z$, then it also has such a representation with the stronger requirement $n_i \geq \theta + 1$. For $\theta > z$ the groups G may thus be identified with each other.

In particular $Q^*/\Gamma(n^2 + 1)$ is free for all θ.

LEMMA 2. *Let $Q(x) = bx^2 + a$ with integers $b > 0$ and $a \neq 0$. There are positive integers D_0, D, D_i, $i = 1, 2, 3$, so that*

$$a^2 Q(D_0 x Q(Dx)) = Q(D_1 x) Q(D_2 x) Q(D_3 x).$$

PROOF. The strategy behind this lemma is to compose a quadratic polynomial with a cubic polynomial in such a way that the resulting polynomial splits into three quadratics. Consideration of algebraic extensions of the rationals shows that the cubic must be reducible.

Consider $Q(M^{-1}x(bx^2 + a) + x)$ where M may be thought of as a rational number. It has the alternative representation

$$M^{-2} Q(x)(b^2 x^4 + bx^2[a + 2M] + M^2).$$

The polynomial of degree 4, considered as a quadratic in bx^2, is reducible if $(a + 2M)^2 - 4M^2$ is a square. Choosing M to be of the form $a(\rho^2 - 1)/4$ for a rational ρ will ensure that this condition is satsified, and the polynomial splits as

$$[bx^2 + a(\rho + 1)^2/4][bx^2 + a(\rho - 1)^2/4].$$

With this choice of M, $M + a = a(\rho^2 + 3)/4$. Here $\rho^2 + 3 = y^2$ has only $\rho = \pm 1$, $y = \pm 2$ as integral solutions, but has infinitely many rational solutions given by $\rho = \frac{1}{2}(3t - 1/t)$, $y = \frac{1}{2}(3t + 1/t)$. It is convenient to note that $\rho > 0$ if $t > 1/\sqrt{3}$; and that since $2t(\rho - 1) = (3t + 1)(t - 1)$ for positive rational values of t, $\rho > 1$ if and only if $t > 1$.

Noting further that

$$bx^2 + a\left(\frac{\rho - 1}{2}\right)^2 = \left(\frac{\rho - 1}{2}\right)^2 Q\left(\frac{2x \operatorname{Sign} a}{\rho - 1}\right)$$

where

$$\operatorname{Sign} a = \begin{cases} 1 & \text{if } a > 0, \\ -1 & \text{if } a < 0, \end{cases}$$

we obtain the identity

$$a^2 Q\left(\frac{x(3t + 1/t)^2}{4M} Q\left(\frac{2x}{3t + 1/t}\right)\right) = Q(x) Q\left(\frac{2x}{\rho + 1}\right) Q\left(\frac{2x \operatorname{Sign} a}{\rho - 1}\right).$$

We set

$$x = (a/4)(\rho^2 - 1)(3t + 1/t)(2t)^r z$$

and fix r at a value sufficiently large that all the polynomials belong to $Z[t, z]$. If $a > 0$, we choose t to be a rational number exceeding 1, if $a < 0$, we choose t to be a rational number in the interval $1/\sqrt{3} < t < 1$. This ensures that both ρ and $a(\rho - 1)$ are positive. Replacing z by $D_4 u$ for a suitably chosen positive integer D_4 we obtain the desired identity with u in place of x.

It is interesting that the constants D and D_i, $i = 1, 2$, are constant multiples of a, while D_3 is a constant multiple of $|a|$. D_0 is an absolute constant. They satisfy $|a| D_0 D^2 = D_1 D_2 D_3$.

Other examples in the persistence of form of quadratic polynomials are given in [5].

4. Proof of Theorems 1 and 2 for $x^{-1}(bx^2 + a)$.

LEMMA 3. *Let $g = k(k + 2l)(k, l)^{-1}$. There are polynomials K_i in $Z[x]$ with positive leading coefficients and of degree at most 3, so that*

$$x^g = \prod_{i=1}^{c} w(K_i)^{\varepsilon_i}, \quad \varepsilon_i = \pm 1.$$

PROOF. Raising the identity of Lemma 2 to the lth power gives

$$x^{-3k} \prod_{i=1}^{3} D_i^{-k} w(D_i x) = a^{2l} (D_0 x Q(Dx))^{-k} w(D_0 x Q(Dx)).$$

In turn we take $l(k, l)^{-1}$ powers in this equation and obtain a representation

$$x^g L = \prod_{i=1}^{h} w(J_i(x))^{\varepsilon_i}$$

with a positive constant L and polynomials $J_i(x)$ in $Z[x]$, of degree at most 3, with positive leading coefficients.

Employing this identity twice, once with $x = 1$, gives the desired identity of Lemma 3.

In the application of Lemma 3 it is sometimes convenient to be able to assert that all integer specializations of the polynomials K_i exceed a given constant. This may be obtained by replacing x in the above identity involving the $J_i(x)$ with Ex for a suitable integer E, or by also employing the identity with x everywhere replaced by x^2.

In the case $-k = 1 = l$ we have $g = 1$, giving the triviality of $H(x^{-1}(bx^2 + a))$, and so that of $Q^*/\Gamma(n^{-1}(bn^2 + a))$ for all θ. For the cubics $x(x^2 + a)$ we obtain $g = 3$.

5. In this and all following sections the relation $g_1 \sim g_2$ between two members of a group G means that their ratio $g_1 g_2^{-1}$ belongs to the kernel of a given group homomorphism $G \to H_1$, or of a composition of homomorphisms $G \to H_1 \to H_2 \to \cdots$.

We shall apply, many times, the identity

$$B(B(x) + x) = B(x)B(x + 1) \tag{1}$$

which is valid for all quadratic polynomials $B(x)$ in $Z[x]$ which are of the form $x^2 + \beta x + \gamma$. It is the case $\alpha = 1 = M$ of Lemma 1.

In this section and until further notice $b = 1$ *so that* $w(x) = x^k(x^2 + a)^l$.

LEMMA 4. *Under the map* $Q(x^*) \to H(w(x))$ *we have* $(x^2 + a - 1)^{kls} \sim (x^2 - 1)^{kls}$ *with* $s = (k, l)^{-1}$.

PROOF. Beginning with the relation $(x^2 + a)^l \sim x^{-k}$ we apply identity (1) with $B(x) = x^2 + a$ to obtain

$$(x^2 + x + a)^{-k} \sim (B(x^2 + x + a))^l \sim (x(x + 1))^{-k}.$$

Using the left and right ends of this expression and applying identity (1), this time with $B(x) = x^2 + x + a$, yield

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

We replace x by $x - 1$ and eliminate between the resulting expression and the first relation to obtain

$$(x^2 + a - 1)^{kls} \sim (x^2 - 1)^{kls} x^{ks(k+2l)}.$$

An application of Lemma 3 now gives the desired result.

LEMMA 5. *Let* $\beta = kl(k, l)^{-1}$. *Under the composition of maps* $Q(x)^* \to H(w(x)) \to \beta H(w(x))$ *we have*

$$x^2 + x + a - m^2 + m \sim (x - m + 1)(x + m), \tag{2}$$

$$x^2 + a - m^2 \sim (x - m)(x + m) \tag{3}$$

for $m = 1, 2, \ldots$.

The second homomorphism in this sequence raises elements to their βth power.

PROOF. The proof goes by induction, following the procedure (3) for m implies (2) for $m + 1$ implies (3) for $m + 1$.

For $m = 1$ the assertion is guaranteed by Lemma 4.

Suppose now that (2), (3) hold for an $m \geq 2$. Applying the identity (1) with $B(x) = x^2 + a - m^2$ we have

$$(x^2 + x + a - m^2 - m)(x^2 + x + a - m^2 + m) = (B(x) + x - m)(B(x) + x + m)$$
$$\sim B(B(x) + x) = B(x)B(x+1) \sim (x - m)(x + m)(x + 1 - m)(x + 1 + m).$$

This together with the induction hypotheses (2) for m shows that

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

which is (2) for $m + 1$.

To continue, apply identity (1) with $B(x)$ the polynomial on the left side of this relation. Then

$$\begin{aligned}(x - m)(x + 1 + m)(x + 1 - m)(x + 2 + m) &\sim B(x)B(x+1)\\ &= B(B(x) + x) \sim (B(x) + x - m)(B(x) + x + 1 + m)\\ &= ((x+1)^2 + a - (m+1)^2)((x+1)^2 + a - m^2),\end{aligned}$$

and (3) for $m + 1$ follows if we replace x by $x - 1$ and apply (3) for m.

The proof of Lemma 5 is complete.

LEMMA 6. *Let the situation of Lemma* 5 *be in force. Then there are integers* b_j, $j = 1, \ldots, 4$, *so that* $(x - b_1)(x - b_3)/(x - b_2)(x - b_4) \sim 1$, *where the rational function is not identically* 1.

PROOF. We may clearly assume that -1 is not a square. Suppose first that a is odd or divisible by 4. We can write it in the form $r^2 - s^2$ using $r = (a + 1)/2$, $s = (a - 1)/2$; or $r = (a + 4)/4$, $s = (a - 4)/4$ respectively. From relation (3) of Lemma 5 with $m = |r| \geq 1$ we obtain

$$(x - |s|)(x + |s|)/(|x - |r||)(x + |r|) \sim 1$$

since then $x^2 + a - m^2 = x^2 - s^2$ is reducible.

If a is even but only divisible by 2, it can be expressed in the form $a = (c - k)(c + k - 1)$. One such representation is given by

$$a = a_1 a_2, \quad c = (a_1 + a_2 + 1)/2, \quad k = (a_2 - a_1 + 1)/2$$

provided that a_1, 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 $a_1 = |a|$, $a_2 = \operatorname{Sign} a$ we obtain from Lemma 5(2)

$$(x + k)(x - k + 1)/(x + c)(x - c + 1) \sim 1.$$

This completes the proof of Lemma 6.

6. In this section I show that for squarefree g one can simplify the relation in Lemma 5 by acting upon a distinguished subgroup of $H(w(x))$ with a suitable ring of operators. The procedure is somewhat general.

Let r be a positive integer, and let M be the subgroup of $Q(x)^*$ generated by the first r integers and the polynomials $w(P)$, where P belongs to $Z[x]$ and has positive leading coefficient. Thus M is possibly a little large than $\Delta(w(x))$. Let H_1 be the quotient group $Q(x)^*/M$, and let τ be the canonical homomorphism $Q(x)^* \to H_1$.

Let Y be the subgroup of $Q(x)$ generated by the positive integers and the rational functions of the form

$$\psi(x) = \prod_{i=1}^{k} (x + c_i)^{d_i}$$

with integers c_i, d_i. Note that for any integer l, the operation $\psi(x) \mapsto \psi(x + l)$ takes Y into itself. *In this section $\tau(Y)$ will be written additively.*

We introduce a shift operator E to act on $\tau(Y)$ by $E^t\tau(x + b) = \tau(x + b + t)$, and by linearity extend the definition so that the polynomial ring $F_g[E]$ acts upon $\tau(Y)$, where F_g is the residue class ring Z/gZ. The g-torsion derived in Lemma 3 ensures that this action is well defined.

If, in the notation of Lemma 6, $b = \max |b_i|$, $1 \leq i \leq 4$, then we have

$$\sum_{i=1}^{4} (-1)^{i+1} E^{b-b_i} \tau(x) = 0. \tag{4}$$

LEMMA 7. *Assume that g is squarefree. If r is fixed at a large enough value, then there is an integer t so that $(E - 1)^t \tau(x) = 0$.*

PROOF. To begin with assume that g is a prime, so that $F = F_g$ is a field. Those operators in $F(E)$ which annihilate $\tau(x)$ form an ideal, nontrivial because it contains the polynomial at (4). Since F is a field, this ideal is principal, generated by $\phi(E)$ say. We factorize this generator in a suitable algebraic extension of F,

$$\phi(z) = \prod_{i=1}^{s} (z - \omega_i)^{r_i},$$

with distinct roots ω_i.

For each positive integer d define

$$\phi_d(z) = \prod_{i=1}^{s} (z - \omega_i^d)^{r_i}.$$

Since the coefficients of this polynomial are symmetric functions of the ω_i, they are functions of the coefficients of $\phi(z)$. Thus $\phi_d(z)$ belong to $F[z]$. Moreover, for each value of i

$$\frac{z^d - \omega_i^d}{z - \omega_i} = z^{d-1} + z^{d-2}\omega_i + \cdots + \omega_i^{d-1},$$

so that $\phi_d(z^d)/\phi_d(z)$ is a polynomial with coefficients in an extension field of F. It is clear that these coefficients must actually belong to F. It follows that

$$\phi_d(E^d)\tau(x) = 0. \tag{5}$$

Let

$$\phi_d(z) = \sum_{m=0}^{k} b_m z^m.$$

Then replacing x in (5) by dx gives (assuming that $d \leq r$)

$$\phi_d(E^d)\tau|\, dx = \sum_{m=0}^{k} b\tau(dx + md) = \sum_{m=0}^{k} b_m \tau(x + m),$$

since τ is a homomorphism. In other words, $\phi_d(E)$ also annihilates $\tau(x)$.

Since $\phi(E)$ is of minimal degree in the annihilating ideal, it must coincide with $\phi_d(E)$. In particular, the map $\omega \mapsto \omega^d$ permutes the roots of $\phi(z)$. Let

$$\omega_i \mapsto \sigma\omega_i \mapsto \sigma^2\omega_i \mapsto \cdots \mapsto \sigma^h\omega_i = \omega_i$$

be a cycle in the permutation. Then $\omega_i^{d^h-1} = 1$. We can do this for each root, and obtain an integer δ so that every $\omega_i^\delta = 1$.

If $\delta \leq r$, then $\phi_\delta(E)$ annihilates $\tau(x)$, and $\phi_\delta(E) = (E-1)^v$ with $v = r_1 + \cdots + r_s$.

Suppose now that g is squarefree, with prime-divisors p_i, $i = 1, \ldots, l$. The canonical homomorphisms $H_1 \to H_1/p_iH_1$ show that H_1 is isomorphic to a direct sum of the H_1/p_iH_1, $i = 1, \ldots, l$. For each prime p_i we may prolong τ to the composition $\tau_i: Q(x)^* \to H_1 \to H_1/p_iH_1$, and, with $F_{p_i}(E)$ acting on $\tau_i(Y)$, obtain an integer t_i for which $(E-1)^{t_i}\tau_i(x) = 0$. With $t = \max t_i$, $1 \leq i \leq l$, $(E-1)^t\tau(x)$ projects onto zero in each H_1/p_iH_1, $i = 1, \ldots, l$.

The assertion of the lemma is justified.

LEMMA 8. *Under the conditions of Lemma 7, $t = 1$ may be taken.*

PROOF. Let p be a prime. Iterations of the map $\mu: m \mapsto (m + p - u)/p$ when $m \equiv u \pmod p$, $0 \leq u \leq p-1$, take every positive integer ultimately to 1. Note that $p\mu(m) > m$.

Suppose that, in the notation of Lemma 7, $(E-1)^m\tau_i(x) = 0$. By introducing extra factors $E-1$ we reach $(E-1)^{p_i\mu(m)}\tau_i(x) = 0$, from which $(E^{p_i}-1)^{\mu(m)}\tau_i(x) = 0$ may be deduced by applying the p_i torsion of H_1/p_iH_1. Replacing x by p_ix, and arguing as in the earlier part of the proof of Lemma 7, gives $(E-1)^{\mu(m)}\tau(x) = 0$. Thus the m in our hypothesis can be replaced by $\mu(m)$ and, after enough iterations of μ, by 1.

The projection of $(E-1)\tau(x)$ onto each H_1/p_iH_1 is trivial, and the proof of Lemma 8 is complete.

REMARK. In order to obtain analogues of the results of this section when g is not squarefree, it would be necessary to examine the nature of the annihilating polynomial at (4) when viewed over the rings $Z/p_i^{\alpha_i}Z$, where $p_i^{\alpha_i}$ runs through the exact prime-power divisors of g.

7. Proof of Theorems 1 and 2 for $x(x^2+a)$. In this section $w(x) = x(x^2+a)$. From Lemma 6 there is a representation

$$R(x) = \frac{(x-b_1)(x-b_3)}{(x-b_2)(x-b_4)} = \prod_{i=1}^{j} w(P_i)^{\varepsilon_i}$$

where the rational function $R(x)$ is nontrivial, and the polynomials P_i in $Z[x]$ have positive leading coefficients. Note that here $\beta = 1$.

As mentioned in §1, the group $Q^*/\Gamma(R(n))$ is trivial for all θ, and from this the triviality of $Q^*/\Gamma(n(n^2+a))$ may now be deduced. However, we shall argue via the group $H(x(x^2+1))$.

In the present circumstances $g = 3$, is squarefree. From Lemma 8 we obtain a representation

$$\frac{x-1}{x} = \lambda \prod_{i=1}^{k} w(F_i)^{\varepsilon_i}$$

with $F_i = F_i(x)$ in $Z[x]$, and some rational number λ. Without loss of generality we may assume that no F_i is a constant. Replacing x by x^2 and forming the ratio of the two relations gives another of the form,

$$\frac{x+1}{x} = \prod_{i=1}^{s} w(G_i)^{\varepsilon_i}, \tag{6}$$

with G_i in $Z[x]$ and of positive degree.

For each integer n there is a least integer b so that $n+b$ is a cube. We may apply the representation (6) with $x = n, n+1, \ldots, n+b-1$ in turn, and then employ Lemma 3, to obtain both the independence of $Q^*/\Gamma(n(n^2+a))$ of θ, and its triviality.

For any polynomial $P(x)$ in $Q(x)^*$ relation (6) shows that with respect to the canonical map $Q(x)^* \to H(x(x^2+a))$ we have $P(x) \sim P(x)-1$. Proceeding by induction we obtain $P(x) \sim P(x) - P(0)$, the latter being a polynomial which has a factor x. Thus $P(x) \sim \gamma x^s$ for some constant γ and integer s, $0 \le s \le 2$. From the triviality of $Q^*/\Gamma(n(n^2+a))$ we have $\gamma \sim 1$, and $H(x(x^2+a))$ is clearly cyclic of order 3, generated by the image of x.

8. $G_k = Q^*/\Gamma(n^k(n^2+1))$, and other groups. As a result of my earlier work with the groups $Q^*/\Gamma(F(n))$ I had postulated that such groups might satisfy the conjecture (ii) so long as $F(x)$ were not the power of another rational polynomial. (See Elliott [**4**, in particular Problem 12 on p. 419].) After a lecture on this subject matter which I gave at Oberwolfach, Germany, in October 1984, Lenstra (with a modification of my argument establishing the freedom of $Q^*/\Gamma(n^2+1)$ when $\theta = 0$) and Schinzel showed that the group here denoted by G_2 contains infinitely many independent torsion elements.

Using the above result I here completely determine the groups G_k, $|k| > 1$. In this case Lemma 6, with $\beta = k$, shows that

$$R(x)^k = \left(\frac{(x-b_1)(x-b_3)^k}{(x-b_2)(x-b_4)}\right)^k$$

has a product representation by the $w(P_i)$ with $w(z) = z^k(z^2+a)$, P_i in $Q(x)^*$. From the triviality of $Q^*/\Gamma(R(n))$ we see that with respect to the canonical map $Q^* \to G_k$ we have $m^k \sim 1$ for every positive integer m. Since trivially $m^k(m^2+1) \sim 1$, we also have $m^2+1 \sim 1$ for all m.

The primes 2 and p, $p \equiv 1 \pmod 4$ have product representations by the m^2+1, and are thus equivalent to 1. The primes q, $q \equiv 3 \pmod 4$ satisfy $q^k \sim 1$. Suppose now that a selection of them satisfy

$$\prod_{i=1}^{s} q_i^{\alpha_i} = \prod_{j=1}^{r} (n_j^k(n_j^2+1))^{\varepsilon_j}$$

for positive integers n_j, and integers α_i, $0 \le \alpha_i \le k-1$. Here each q_i must divide a factor n_j^k on the right side, and so α_i must be a multiple of k. This forces $\alpha_i = 0$.

It is clear that G_k is a direct sum of cyclic groups of order k, one generated by the image of each prime q, $q \equiv 3 \pmod 4$. An elaboration of the argument given for $Q^*/\Gamma(n^2+bn+c)$ shows that the groups G_k are independent of θ.

Similar arguments show that all the groups $Q^*/\Gamma(x(x^2+a)^l)$ are trivial.

Perhaps analogues of conjectures (i) and (ii) hold when $F(x)$ is replaced by (say) an absolutely irreducible polynomial in several variables, and Γ is the subgroup generated by its values at suitably restricted points with integer coordinates.

9. Some applications. Suppose that χ is a noncubic, nonprincipal Dirichlet character, defined to some prime modulus p, which satisfies $\chi(n(bn^2+a)) = 0$ or 1 for $n \leq M < p$. Applying Lemma 3 with $k = l = 1$ we see that the nonprincipal character χ^3 has value 1 on the positive integers not exceeding $c_2 M^{1/3}$ for some positive constant c_2 which depends at most upon a, b. A device of Vinogradov (see Burgess [**1**]) in combination with the character sum estimate

$$\left|\sum_{m\leq H} \chi(m)\right| \leq d_r H^{1-1/(r+1)} p^{1/4r} \log p, \qquad r = 1, 2, \ldots,$$

of Burgess [**2**] now shows that $c_2 M^{1/3} > p^\tau$ with a fixed $\tau > (4\sqrt{e})^{-1}$ cannot hold for all large primes p.

If $\lambda > 3(4\sqrt{e})^{-1}$ and the constant c is chosen suitably depending only upon a, b and λ, then the interval $[1, cp^\lambda]$ contains an integer n for which $\chi(n(bn^2+a)) \neq 0, 1$. Since $3(4\sqrt{e})^{-1} = .456\ldots$ this restriction on λ improves upon the condition $\lambda > 1/2$ which may be deduced from a straightforward application of Weil's estimate for

$$\sum_{n=0}^{p-1} \chi(n(bn^2+a)) \exp(2\pi i n k p^{-1}).$$

This improves upon a result of Burgess [**3**] except when χ is a cubic character or $w(x)$ has the particular form $x(x^2 - s(s+1))$ for some integer s.

Let $w(x) = x(x^2+a)$, $a \neq 0$. It follows from (6) in §7 that for every pair of positive integers m, k, there is a representation of the form

$$m = \prod_i w(n_i)^{\varepsilon_i}, \qquad \varepsilon_i = \pm 1,$$

with $k < n_i \leq cm^d$, for certain constants d (depending upon a) and c (depending upon a and k). Suppose now that $\psi(p)$ for a prime p denotes the least positive integer n for which a fixed nonprincipal character χ (cubic or not) satisfies $\chi(n(n^2+a)) \neq 0, 1$. Then this product representation together with Theorem 3 of my paper [**7**] show that as $y \to \infty$

$$\frac{\log y}{y} \sum_{p\leq y} \psi(p) \to \mu$$

for some constant μ. By a fixed character $(\mathrm{mod}\, p)$ is meant a Dirichlet character which is defined in terms of power-residue symbols (cf. Elliott [**7**]). An example is the Legendre symbol $\frac{n}{p}$.

Similar results may be obtained involving the rational function $x^{-1}(bx^2+a)$. Thus if $\lambda > 3(4\sqrt{3})^{-1}$ and the constant c_3 is chosen suitably, every interval $[1, c_3 p^\lambda]$ contains an integer n at which a nonprincipal character χ $(\mathrm{mod}\, p)$ satisfies $\chi(bn + a\bar{n}) \neq 0, 1$, where $n\bar{n} \equiv 1 \ (\mathrm{mod}\, p)$.

REFERENCES

1. D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika **4** (1957), 106–112.
2. ____, *On character sums and primitive roots*, Proc. London Math. Soc. **12** (1962), 179–192.
3. ____, *Dirichlet characters and polynomials*, Proc. Internat. Conf. in Number Theory (Moscow, 14–18 Sept. 1971), Trudy Mat. Inst. Steklov **132** (1973), 203–205.
4. P. D. T. A. Elliott, *Arithmetic functions and integer products*, Grundlehren Math. Wiss., Springer-Verlag, New York and Berlin, 1984.
5. ____, *The value distribution of reducible cubics*, Canad. Math. Bull. **28** (1986), 328–336.
6. ____, *On representing integers as products of integers of a prescribed type*, J. Austral. Math. Soc. (Ser. A) **35** (1983), 143–161.
7. ____, *On the mean value of $f(p)$*, Proc. London Math. Soc. **21** (1970), 28–96.
8. R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge Univ. Press, London, 1981.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO, BOULDER, COLORADO 80309