A Note on the Discriminator

Michael Zieve*
Hill Center, Department of Mathematics, Rutgers University,
110 Frelinghuysen Road, Piscataway NJ 08854
zieve@math.rutgers.edu

Abstract

For $f(X) \in \mathbb{Z}[X]$, let $D_f(n)$ be the least positive integer k for which $f(1), \dots, f(n)$ are distinct modulo k. Several results have been proven about the function D_f in recent years, culminating in Moree's characterization of $D_f(n)$ whenever f lies in a certain (large) subset of $\mathbb{Z}[X]$ and n is sufficiently large. We give several improvements of Moree's result, as well as further results on the function D_f.

1 Introduction

Let $f(X) \in \mathbb{Z}[X]$ be a polynomial over the integers. For any positive integer n, let $D_f(n)$ denote the least positive integer k such that $f(1), \dots, f(n)$ are distinct modulo k. If no such k exists, we put $D_f(n) = \infty$. The function D_f has been called the 'discriminator', since it represents the least modulus which discriminates the consecutive values of the polynomial f. This function was originally studied for cyclic polynomials $f = X^d$, in which case the main result is due to Bremser, Schumer and Washington [2]. When d is odd they showed that, for any sufficiently large n, $D_f(n)$ is the least integer $k \geq n$ for which the induced mapping $f\colon \mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ is a permutation. This result can be interpreted as saying that no polynomial $f(X) = X^d$, with d odd, can 'almost' permute $\mathbb{Z}/k\mathbb{Z}$ for large k; for, if the first several values of f are distinct modulo k, the result shows that f must in fact permute $\mathbb{Z}/k\mathbb{Z}$. Subsequent work showed that a similar conclusion can be drawn

*The author's work supported by an NSF predoctoral fellowship

for other types of polynomials f. Moree and Mullen [11] extended the above result to the case where f is a Dickson polynomial of degree coprime to 6. The Dickson polynomial of degree $d \geq 1$ and parameter $a \in \mathbb{Z}$ is defined to be the unique polynomial $g_d(X, a) \in \mathbb{Z}[X]$ for which $g_d(X + a/X, a) = X^d + (a/X)^d$; explicitly,

$$g_d(X, a) = \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-a)^i X^{d-2i}.$$

Since $g_d(X, 0) = X^d$, the Dickson polynomials generalize the cyclic polynomials.

Subsequently Moree [10] extended these results to a larger class of polynomials f. We give some notation before stating his result. Let $V_f(k) = |\{f(c) \colon c \in \mathbb{Z}/k\mathbb{Z}\}|$ be the cardinality of the value set of f over $\mathbb{Z}/k\mathbb{Z}$. Define $S(f) = \sup\{V_f(p)/p \colon p \text{ prime}, V_f(p) < p\}$ and $C(f) = \max\{2/3, S(f)\}$; if $V_f(p) = p$ for every prime p, or equivalently if $f(X) = b \pm X$, put $S(f) = 0$ and $C(f) = 2/3$. If every sufficiently large integer n has the property that the interval $[n, n/C(f)]$ contains an integer k for which f permutes $\mathbb{Z}/k\mathbb{Z}$, then let $n_0(f)$ denote the least integer ≥ 4 such that every $n \geq n_0(f)$ has this property.

Theorem 1 (Moree) *Suppose $n_0(f)$ exists. Then, for every $n \geq n_0(f)$,*

$$D_f(n) = \min\{k \geq n \colon f \text{ permutes } \mathbb{Z}/k\mathbb{Z}\}. \tag{1}$$

From the above discussion it is apparent that the behavior of D_f is related to the set $\mathcal{Q}(f) = \{q \geq 1 \colon f \text{ permutes } \mathbb{Z}/q\mathbb{Z}\}$. For, if $n \leq q$ and $q \in \mathcal{Q}(f)$, then certainly $f(1), \ldots, f(n)$ are distinct modulo q:

$$D_f(n) \leq \min\{q \colon q \geq n,\ q \in \mathcal{Q}(f)\}.$$

In the other direction, it is clear that $D_f(n) \geq n$; so (1) simply asserts that $D_f(n) \in \mathcal{Q}(f)$. In general, if there are elements of $\mathcal{Q}(f)$ only slightly greater than n, then the least such element is a good candidate for $D_f(n)$. This leads us to consider the distribution of the elements of $\mathcal{Q}(f)$; a fundamental quantity is

$$\gamma(f) = \limsup_{i \to \infty} q_{i+1}/q_i,$$

where $q_1 < q_2 < q_3 < \ldots$ denote the elements of $\mathcal{Q}$ written in increasing order. If $\mathcal{Q}(f)$ is finite, we put $\gamma(f) = \infty$. We study $\gamma(f)$ in the next section.

In this note we make several improvements to Moree's result. Continuing the theme of previous developments, we show that the conclusion of this result remains valid for a larger class of polynomials f. Note that Theorem 1 applies only when $\gamma(f) \leq 1/C(f) \leq 3/2$; our first priority is to improve the number $3/2$ in this result. In Section 3 we find that, essentially, we can replace the $3/2$ by 2; and in Section 5 we show that there would be counterexamples if we replaced $3/2$ by any number greater than 2. Next, the 'sup' in the definition of $S(f)$ is somewhat unnatural, since it places undeserved importance on special behavior modulo small primes; in Section 4 we show that the 'sup' can be replaced by 'limsup'. In a different direction, we study the values of $D_f(n)$ when n is small; we improve the constant $n_0(f)$, give criteria for small values of $D_f(n)$ to lie in $\mathcal{Q}(f)$, and provide information about the prime factorizations of values of $D_f(n)$ lying outside $\mathcal{Q}(f)$. We carefully analyze several examples, which illustrate various phenomena. In the final section we mention two generalizations of discriminators.

Finally we comment on notation. Throughout this note, the letter p is reserved for prime numbers. Greek letters denote real numbers and calligraphic letters denote sets. The elements of $\mathcal{Q}(f)$, in increasing order, are always denoted $q_1 < q_2 < \dots$.

2 Some results on $\gamma(f)$

In this section we give some preliminary information on $\gamma(f)$. Before doing this we recall some simple facts about $\mathcal{Q}(f)$.

Lemma 2 *(i) If $q \in \mathcal{Q}(f)$ and $k \mid q$, then $k \in \mathcal{Q}(f)$.*
(ii) For a, b coprime positive integers, $ab \in \mathcal{Q}(f)$ if and only if $a, b \in \mathcal{Q}(f)$.
(iii) For p prime, the following are equivalent:

(1) $p^2 \in \mathcal{Q}(f)$;

(2) $p^\ell \in \mathcal{Q}(f)$ for every $\ell \geq 1$;

(3) $p \in \mathcal{Q}(f)$ and $f'(X)$ has no roots in $\mathbb{Z}/p\mathbb{Z}$.

Proof. *(i)* is trivial, *(ii)* follows from the Chinese Remainder Theorem, and *(iii)* is [9, Cor. 4.3]. ■

It is convenient to partition the set $\mathbb{Z}[X]$ into three disjoint sets: $\mathbb{Z}[X] = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$. The set $\mathcal{C}_3$ consists of the polynomials f for which $\mathcal{Q}(f)$ is finite; by the above lemma, a polynomial f lies in $\mathcal{C}_3$ if and only if $\mathcal{Q}(f)$ contains only finitely many primes and no squares of primes. The set $\mathcal{C}_2$ consists of the polynomials f for which $\mathcal{Q}(f)$ contains only finitely many primes, and precisely one square of a prime. The set $\mathcal{C}_1$ contains all remaining $f \in \mathbb{Z}[X]$. We write $\mathcal{C}_1 = \mathcal{A} \cup \mathcal{B}$, where $f \in \mathcal{A}$ whenever $\mathcal{Q}(f)$ contains infinitely many primes, and $f \in \mathcal{B}$ whenever $\mathcal{Q}(f)$ contains the squares of two or more primes. Note that $\mathcal{A}$ and $\mathcal{B}$ are not disjoint, since for instance they both contain the polynomial X (it can be shown that both sets contain $g_d(X, a)$ whenever $a \neq 0$ and $(d, 6) = 1$). Note that our $\mathcal{C}_1$ and $\mathcal{C}_2$ differ from those in [10].

We now discuss the values of $\gamma(f)$ for f in each of the subsets of $\mathbb{Z}[X]$ defined above. We will see that $\gamma(f) = 1$ if and only if $f \in \mathcal{C}_1$. Note that the set $\mathcal{C}_3$ is trivial here, since $\gamma(f)$ is defined to be ∞ when $f \in \mathcal{C}_3$.

Lemma 3 *$\gamma(f) = 1$ for every $f \in \mathcal{A}$.*

In our proof, we will need to know which rings $\mathbb{Z}/p\mathbb{Z}$ are permuted by a Dickson polynomial. It is well known that, for $a \in \mathbb{Z}$ and d an odd prime, $g_d(X, a)$ permutes $\mathbb{Z}/p\mathbb{Z}$ if and only if either $d \nmid p^2 - 1$, or both $d \nmid p - 1$ and $p \mid a$; see for instance [9, Thm. 4.5]. The following proof is an elaboration of two sentences from Section 3.1 of [10], and clarifies certain details obscured there.

Proof. This is an easy consequence of a theorem of M. Fried [6], known as Schur's Conjecture. For further discussion of this result see [9, Ch. 6]. Now, suppose $f \in \mathcal{A}$. By [9, Cor. 6.23], f is the composition of linear polynomials in $\mathbb{Q}[X]$ and Dickson polynomials $g_d(X, a)$ with $a \in \mathbb{Z}$ and d an odd prime (and $a = 0$ if $d = 3$). Let D be the product of all the distinct primes occurring as some d in this decomposition; thus, D is the product of the distinct prime divisors of the degree of f. Consider any prime $p \equiv 2 \pmod{D}$. For any such p, each $g_d(X, a)$ in the decomposition permutes $\mathbb{Z}/p\mathbb{Z}$: for, we have $p \equiv 2 \pmod{d}$, so $p^2 - 1 \equiv 3 \pmod{d}$, whence $d \nmid p^2 - 1$ unless $d = 3$, in which case $a = 0$ and $d \nmid p - 1$. And for all but finitely many of these primes p, each of the linear polynomials in the decomposition permutes $\mathbb{Z}/p\mathbb{Z}$. Thus, for all sufficiently large primes $p \equiv 2 \pmod{D}$, f permutes $\mathbb{Z}/p\mathbb{Z}$. Since D is odd, there are infinitely many primes $p \equiv 2 \pmod{D}$, by Dirichlet's Theorem on arithmetic progressions; write these primes as $p_1 < p_2 < \ldots$. By the Prime Number Theorem for arithmetic progressions [5, Chaps. 20 and 22], we have

$\lim_{i\to\infty} p_{i+1}/p_i = 1$; it follows that $\gamma(f) = \limsup_{i\to\infty} q_{i+1}/q_i = 1$, and the lemma is proved. ■

Lemma 4 *$\gamma(f) = 1$ for every $f \in \mathcal{B}$.*

This is essentially Lemma 4 of [10]. The quick proof given there relies on only elementary properties of continued fractions.

The case $f \in \mathcal{C}_2$ is more difficult. In [10], $\gamma(f)$ is calculated in this case by means of a certain graph. Our next lemma gives a simpler, more direct approach. This requires some notation. Let q be the prime whose square is in $\mathcal{Q}(f)$, and let $p_1, \dots, p_s$ be the other primes in $\mathcal{Q}(f)$. Put $P = \prod_{i=1}^{s} p_i$. Note that $\mathcal{Q} = \{kq^\ell : \ell \geq 0,\ k \mid P\}$. Recall that we write the elements of $\mathcal{Q}$ as $q_1 < q_2 < \dots$.

Lemma 5 *For $f \in \mathcal{C}_2$, we have $\gamma(f) > 1$; in fact, if $q_b = qq_a$ and $P < q_b$, then $\gamma(f) = \max_{a\leq i<b} q_{i+1}/q_i$.*

Proof. Note that an integer $m > P$ lies in $\mathcal{Q}(f)$ if and only if $m/q \in \mathcal{Q}(f)$. Thus, $q_{i+b-a} = qq_i$ whenever $i \geq a$; hence, for $i \geq a$, we have $q_{i+1}/q_i = q_{i+b-a+1}/q_{i+b-a}$. From this the result follows. ■

One consequence of the above lemmas is the result stated before them.

Proposition 6 *For $f \in \mathbb{Z}[X]$, $\gamma(f) = 1$ if and only if $f \in \mathcal{C}_1$.*

Next we show that, if $\gamma(f) = 1$, then $D_f(n) \in \mathcal{Q}(f)$ for all sufficiently large n. This follows from Theorem 1 once we know that $S(f) < 1$. In [10] Moree proved $S(f) < 1$ by appealing to Wan's value set bound from [14]. One could also show $S(f) < 1$ by citing Cohen's results from [4]; there he showed that $V_f(p) = \alpha p + O(\sqrt{p})$, where α depends on f and p but the implied constant depends only on f. Further, Cohen showed that, for fixed f, there are only finitely many possibilities for α, all between 0 and 1; and moreover, if $\alpha = 1$ then $V_f(p) = p$. From these results it follows that $S(f) < 1$, so, for $f \in \mathcal{C}_1$, we have $D_f(n) \in \mathcal{Q}(f)$ whenever n is sufficiently large. Thus the interesting case, so far as the behavior of $D_f(n)$ for sufficiently large n is concerned, is $f \in \mathcal{C}_2$. Theorem 1 applies to some of these f; in the next two sections we give results which apply to many more f.

Finally, we discuss the possible values of $\gamma(f)$. The above results show that $\gamma(f) = q^\ell a/b$, where q is prime, $\ell \in \mathbb{Z}$, and a, b are squarefree positive integers; but not every number of this form occurs as the value of $\gamma(f)$ for

some f, since we also know $\gamma(f) \geq 1$ (one can also show, for instance, that $15/8$ does not occur as $\gamma(f)$ for any f). We now show that there are values $\gamma(f)$ arbitrarily close to any prescribed number $\alpha \geq \sqrt{2}$.

Proposition 7 *The set* $\{\gamma(f)\colon f \in \mathcal{C}_2\}$ *contains a dense subset of the interval* $[\sqrt{2}, \infty)$.

Proof. Pick any α, β with $\sqrt{2} < \alpha < \beta$; it suffices to show that $\gamma(f) \in (\alpha, \beta)$ for some $f \in \mathcal{C}_2$. Let q be a prime such that $\alpha < q < \alpha^2$; the existence of q is guaranteed by Bertrand's Postulate when $\alpha \geq 2$, and clearly $q = 2$ suffices when $\alpha < 2$. Pick any δ with $1 < \delta < \min\{\beta/\alpha,\, q/\alpha\}$. The Prime Number Theorem implies that, whenever j is sufficiently large, the interval $(\alpha q^j, \delta\alpha q^j)$ contains a prime p. Fix some such j and p; note that $q^j < p < q^{j+1}$. Suppose some polynomial $f \in \mathcal{C}_2$ has $\mathcal{Q}(f) = \{q^\ell,\, pq^\ell\colon \ell \geq 0\}$. Then Lemma 5 would imply that $\gamma(f) = \max\{p/q^j,\, q^{j+1}/p\}$. Since

$$\frac{q^{j+1}}{p} < \frac{q}{\alpha} < \alpha < \frac{p}{q^j} < \delta\alpha < \beta,$$

we conclude that $\gamma(f) \in (\alpha, \beta)$.

To complete the proof, we must show that some $f \in \mathcal{C}_2$ has $\mathcal{Q}(f) = \{q^\ell,\, pq^\ell\colon \ell \geq 0\}$. Let $d > 1$ be coprime to $p - 1$, and let m be the product of all primes less than d^4 other than p and q. Put $f(X) = m(qX^d + pX)$; it follows from [13] that f does not permute $\mathbb{Z}/r\mathbb{Z}$ for any prime r other than p and q. Clearly $q \in \mathcal{Q}(f)$, and since $(d, p-1) = 1$ we see that also $p \in \mathcal{Q}(f)$. Finally, Lemma 2 implies that $p^2 \notin \mathcal{Q}(f)$ and $q^2 \in \mathcal{Q}(f)$, so indeed $\mathcal{Q}(f) = \{q^\ell,\, pq^\ell\colon \ell \geq 0\}$. ∎

It seems likely that $\{\gamma(f)\colon f \in \mathcal{C}_2\}$ is dense in $[1, \infty)$, but I do not know a proof of this.

3 A 'sup' result

In this section we prove a result involving $S(f) = \sup\{V_f(p)/p\colon V_f(p) < p\}$. We set $S(f) = 0$ if $V_f(p) = p$ for every prime p, which occurs precisely when $f(X) = b \pm X$; in this case $D_f(n) = n \in \mathcal{Q}(f)$ for every n, so all of our results are trivially true. For any polynomial $f \in \mathbb{Z}[X]$, the following result gives information about $D_f(n)$ for some values n. In particular, this result even applies when $f \in \mathcal{C}_3$.

Theorem 8 *Given real numbers $1 < \mu < 2$ and $\nu < 0$ for which $\mu - \mu^2 \le \nu$ and $\mu + \sqrt{\mu^2 - \mu + \nu} < 3$, if the positive integer n satisfies*

$$n = 1 \quad or \quad n \text{ even} \quad or \quad n > \frac{2+\nu}{2-\mu}$$

then either $D_f(n) \in \mathcal{Q}(f)$ or $D_f(n) \ge n/S(f)$ or $D_f(n) > n\mu + \nu$.

This result basically says that, if n is any even number or any sufficiently large odd number, then $D_f(n)$ lies in $\mathcal{Q}(f)$ if it is not too much greater than n. In other words, if there is an element of $\mathcal{Q}(f)$ which is only slightly greater than n, then $D_f(n) \in \mathcal{Q}(f)$.

Corollary 9 *If n, μ, and ν satisfy the hypotheses of the theorem, and the intervals $[n, 1+n\mu+\nu]$ and $[n, 1+ n/S(f))$ each contain an element of $\mathcal{Q}(f)$, then $D_f(n) \in \mathcal{Q}(f)$.*

As a consequence of this corollary, we have an improvement on Theorem 1.

Corollary 10 *Let t be any positive integer, and let $\theta = \max\{S(f), (2t+1)/(4t+1)\}$. For any positive integer n such that both*

(1) either $n = 1$ or n even or $n > 2t$; and

(2) some $q \in \mathcal{Q}(f)$ satisfies $n \le q < n/\theta$,

we have $D_f(n) \in \mathcal{Q}(f)$.

Proof. Let ϵ be a positive real number, and put $\mu = (4t+1)/(2t+1) - \epsilon$ and $\nu = -1$. For any sufficiently small value of ϵ, the present corollary follows from the previous one when we substitute these values of μ and ν. ∎

Already for $t = 1$ we have Theorem 1 with 2/3 improved to 3/5 and 4 improved to 1.

Corollary 11 *If $\gamma(f) < 1/S(f)$ and $\gamma(f) < 2$, then $D_f(n) \in \mathcal{Q}(f)$ for all sufficiently large n.*

With further applications in mind, we state one more result.

Corollary 12 *Suppose $S(f) \le 1/2$. If there is some $q \in \mathcal{Q}(f)$ for which $n \le q \le 2n - 2$, then $D_f(n) \in \mathcal{Q}(f)$.*

Proof. The result is trivial for $n \le 2$, so we only consider $n \ge 3$. Put $\nu = -1$ and $\mu = 2 - \epsilon - 1/n$, where $\epsilon > 0$. When ϵ is sufficiently small, this corollary follows from Corollary 9 upon substituting these values of μ and ν. ∎

This result is fairly general; thus it is somewhat surprising that, even in the well-studied case $f(X) = X^d$ with d odd, it implies the best result known, namely [11, Thm. 3]. For this application one must check that $S(X^d) \le 1/2$, but this follows at once from $V_{X^d}(p) = (p-1)/(d, p-1) + 1$.

We now prove Theorem 8. In our proof we make use of an idea from the proof of [10, Thm. 3]. We will need some simple facts on value sets of polynomials. Clearly $D_f(n) \ge V_f(D_f(n)) \ge n$. Also, if m divides k, then $V_f(m)/m \ge V_f(k)/k$.

Proof of Theorem 8. We prove the contrapositive; so, suppose the conclusion did not hold. Let $k = D_f(n)$; since $k \notin \mathcal{Q}(f)$, $V_f(k) < k$. Let m be the largest squarefree divisor of k. Since $k < n/S(f)$,

$$\frac{V_f(m)}{m} \ge \frac{V_f(k)}{k} \ge \frac{n}{k} > S(f).$$

If $V_f(m) < m$ then, since m is squarefree, there is a prime $p \mid m$ for which $V_f(p) < p$, so $V_f(m)/m \le V_f(p)/p \le S(f)$, a contradiction. Thus $V_f(m) = m$. Since $k \notin \mathcal{Q}(f)$, Lemma 2 implies that some prime power p^ℓ dividing k satisfies $p^\ell \notin \mathcal{Q}(f)$; but $V_f(m) = m$ implies $V_f(p) = p$, so $\ell \ge 2$. By Lemma 2 there is some x_0, with $1 \le x_0 \le p$, for which $f'(x_0) \equiv 0 \pmod p$. Consequently

$$f(x_0 + \frac{k}{p}) \equiv f(x_0) + \frac{k}{p} f'(x_0) \equiv f(x_0) \pmod k,$$

so, by the definition of $k = D_f(n)$, we have $x_0 + k/p \ge n+1$. Our assumption that the theorem's conclusion fails implies that $k \le n\mu + \nu$. Thus

$$n + 1 \le x_0 + \frac{k}{p} \le p + \frac{k}{p} \le p + \frac{n\mu + \nu}{p},$$

so, since $\mu < 2 \le p$, we must have $n \le (p^2 - p + \nu)/(p - \mu)$. It follows from $p^2 \le k \le n\mu + \nu$ that $(p^2 - \nu)/\mu \le n$. Thus

$$\frac{p^2 - \nu}{\mu} \le n \le \frac{p^2 - p + \nu}{p - \mu},$$

so $p^3 - p\nu \le \mu(2p^2 - p)$, or equivalently $p^2 - \nu \le \mu(2p - 1)$. This last inequality implies that $p \le \mu + \sqrt{\mu^2 - \mu + \nu} < 3$, so $p = 2$.

Specializing the facts shown above to the case $p = 2$, we have $n + 1 \le 2 + k/2$ (so $k \ge 2n - 2$) and $4 \mid k$. If $n = 2s$ is even, then $k \ge 4s - 2$ and $4 \mid k$ imply $k \ge 4s$; but $4s \le k \le 2s\mu + \nu < 4s + \nu < 4s$ gives a contradiction. Thus $n = 2s + 1$ is odd; clearly $D_f(1) = 1$, so assume $s > 0$. Here we have $4s \le k \le (2s + 1)\mu + \nu$, or equivalently $2s(2 - \mu) \le \mu + \nu$, so indeed $n = 2s + 1 \le (2 + \nu)/(2 - \mu)$ as desired. ■

The methods of this proof apply even when $\gamma(f) > 2$, in which case they provide information about the prime factorization of the values $D_f(n)$ lying outside $\mathcal{Q}(f)$. For instance, the proof shows that, if $D_f(n) \notin \mathcal{Q}(f)$ and $D_f(n) < n/S(f)$, then $D_f(n)$ is divisible by the square of some prime p; further hypotheses would enable us to give an upper bound on p.

4 A 'limsup' result

We now prove a result involving $L(f) = \limsup\{V_f(p)/p \colon V_f(p) < p\}$. If $V_f(p) = p$ for all but finitely many p, i.e. if $f(X) = aX + b$ with $a \ne 0$, we put $L(f) = 0$; our results become trivial in this case. We begin with two simple lemmas.

Lemma 13 *If $s \mid D_f(n)$, then $V_f(s)/s \ge n/D_f(n)$.*

Proof. We have $V_f(s)/s \ge V_f(D_f(n))/D_f(n) \ge n/D_f(n)$. ■

Lemma 14 *If $D_f(n) = st$, and there exist $0 < a < b \le s$ for which $f(a) \equiv f(b) \pmod{s}$, then $D_f(n) > 2(n - b)$.*

Proof. Consider the set $\mathcal{W} = \{a + si,\, b + si \colon 0 \le i \le t/2\}$. The size of $\mathcal{W}$ is $2(1 + \lfloor t/2 \rfloor) > t$. But, for each $w \in \mathcal{W}$, $f(w) \equiv f(a) \pmod{s}$; since there are only t classes (mod st) which are congruent to $f(a) \pmod{s}$, there must be distinct $x, y \in \mathcal{W}$ for which $f(x) \equiv f(y) \pmod{st}$. Since $D_f(n) = st$, we must have $n < \max\{x, y\} \le b + st/2$, so $D_f(n) = st > 2(n - b)$. ■

These two lemmas give a good deal of information about D_f. They give particularly good information about 'large' values of D_f, as our next theorem indicates. We focus on the polynomials in $\mathcal{C}_2$. For any $f \in \mathcal{C}_2$, there is an integer $N_0(f)$ such that, for any $n \ge N_0(f)$, the interval $[n, n/\gamma(f))$ contains

an element of $\mathcal{Q}(f)$. One can construct such an integer $N_0(f)$ as follows. For $f \in \mathcal{C}_2$, Lemma 5 implies that

$$\gamma(f) = \max_{q_i > N(f)} q_{i+1}/q_i,$$

where $N(f) = P/q$ (here P is the product of the primes in $\mathcal{Q}(f)$ whose squares are not in $\mathcal{Q}(f)$, and q is the prime whose square is in $\mathcal{Q}(f)$). Thus, if $q_i > N(f)$, then $q_{i+1}/q_i \le \gamma(f)$. If I is the least index for which $q_I > N(f)$, let $N_0(f)$ be the least integer greater than $q_I/\gamma(f)$. Then indeed, for any $n \ge N_0(f)$, the interval $[n, n\gamma(f))$ contains an element of $\mathcal{Q}(f)$.

Now we give two more lemmas, the first of which is an immediate consequence of Lemma 13.

Lemma 15 *If $f \in \mathcal{C}_2$ and $n \ge N_0$ then, for any divisor s of $D_f(n)$, we have $V_f(s)/s > 1/\gamma$.*

Lemma 16 *If the prime p lies in $\mathcal{Q}$ but $p^2 \notin \mathcal{Q}$, then there exist a, b such that $0 < a < b \le 2p$ and $f(a) \equiv f(b) \pmod{p^2}$.*

Proof. Lemma 2 implies that there exists x_0, with $1 \le x_0 \le p$, such that $f'(x_0) \equiv 0 \pmod{p}$. Thus

$$f(x_0 + p) \equiv f(x_0) + pf'(x_0) \equiv f(x_0) \pmod{p^2};$$

since $x_0 + p \le 2p$, this proves the lemma. ∎

We are now ready for the main result of this section.

Theorem 17 *Suppose that $1 < \gamma < 2$ and $n \ge N_0$, but $D_f(n) \notin \mathcal{Q}$. Then $D_f(n) = st$, where $t < 2\gamma/(2-\gamma)$ and $s \notin \mathcal{Q}$ is either a prime p for which $V_f(p)/p > 1/\gamma$, or the square of a prime $p \in \mathcal{Q}$ with $p < 4\gamma/(2-\gamma)$.*

Proof. We can certainly write $D_f(n) = st$, where $s \notin \mathcal{Q}$, and by Lemma 2 we may assume that either s is prime, or s is the square of a prime $p \in \mathcal{Q}$. Since $n \ge N_0$, there is an element of $\mathcal{Q}$ in $[n, n\gamma)$, so $D_f(n) < n\gamma$. Let b be the least positive integer for which the interval $(0, b)$ contains an integer a with $f(a) \equiv f(b) \pmod{s}$; since $s \notin \mathcal{Q}$, we know $b \le s$. By Lemma 14, $2(n-b) < D_f(n) < n\gamma$, so $b/n > 1 - \gamma/2$. Thus,

$$t = \frac{D_f(n)}{s} = \frac{D_f(n)}{n}\frac{n}{b}\frac{b}{s} < \gamma\frac{2}{2-\gamma}\frac{b}{s} \le \frac{2\gamma}{2-\gamma}.$$

Lemma 15 implies $V_f(s)/s > 1/\gamma$, so we are done if s is prime. Now let $s = p^2$, where $p \in \mathcal{Q}$. Lemma 16 implies $b \le 2p$, so $2(n-2p) \le 2(n-b)$; from above, $2(n-b) < n\gamma$, so $2(n-2p) < n\gamma$. Thus $n(2-\gamma) < 4p$, so

$$p \le \frac{st}{p} = \frac{D_f(n)}{p} < \frac{n\gamma}{p} < \frac{4\gamma}{2-\gamma},$$

and the proof is complete. ■

For f with $\gamma(f) < 2$, this result gives a great deal of information about the large values of D_f which lie outside $\mathcal{Q}(f)$. In particular, such values must be small multiples of a large prime. This enables us to focus our attention on large primes, rather than arbitrary primes, and hence allows us to improve Corollary 11 by replacing $S(f)$ by $L(f)$.

Corollary 18 *If $L(f)\gamma(f) < 1$ and $\gamma(f) < 2$, then $D_f(n) \in \mathcal{Q}(f)$ for all sufficiently large n.*

Here, for $f \in \mathcal{C}_2$, we say n is 'sufficiently large' if $n \ge N_0(f)$, $D_f(n) \ge (1/2)(4\gamma/(2-\gamma))^3$, and

$$D_f(n) \ge \frac{2\gamma}{2-\gamma} \cdot \max\{p \notin \mathcal{Q}\colon V_f(p)/p > 1/\gamma\}.$$

We now give examples of polynomials $f \in \mathcal{C}_2$ which satisfy the hypotheses of Corollary 18 but not the hypotheses of Theorem 1. It is actually rather difficult to produce explicit examples, since it is usually quite difficult to compute $S(f)$ or $L(f)$. We use a class of polynomials for which $L(f)$ has been computed.

Example. We show that many polynomials $f(X) = m(qX^d + pX)$ satisfy the hypotheses of Corollary 18 but not the hypotheses of Theorem 1. First, pick any α, β with $3/2 < \alpha < \beta < e/(e-1)$; the proof of Proposition 7 produces two primes p and q. That proof shows that, if $d > 1$ is coprime to $p-1$, and m is divisible by every prime less than d^4 except p and q (and moreover $(m, pq) = 1$), then $f(X) = m(qX^d + pX)$ has $\gamma(f) \in (\alpha, \beta)$. Since $\gamma(f) > 3/2$, Theorem 1 does not apply. Next we show that Corollary 18 does apply to some of these polynomials.

To this end, recall that $\sum_{i=1}^{\infty}(-1)^{i-1}/i! = (e-1)/e$; since $\gamma(f) < e/(e-1)$, whenever d is sufficiently large we will have $\alpha_d := \sum_{i=1}^{d}(-1)^{i-1}/i! < 1/\gamma(f)$. Pick any such d (we are still requiring that $(d, p-1) = 1$ and $d > 1$). A

result of Birch and Swinnerton-Dyer [1, Thm. 1, Ex. (i)] says that, for any sufficiently large prime r, we have $V_f(r) = r\alpha_d + O(r^{1/2})$; here the implied constant depends only on d. It follows at once that $L(f) = \alpha_d$, so indeed $L(f) < 1/\gamma(f)$ (and $\gamma(f) < e/(e-1) < 2$), and thus Corollary 18 applies to f.

If we insist that mpq be divisible by each of the first k primes, where k is sufficiently large, then we can force $S(f) < 1/\gamma(f)$ in this example, in which case the polynomials f satisfy the hypotheses of Corollary 11 but not those of Theorem 1.

5 Examples with $\gamma(f) > 2$

In this section we give an infinite family $\mathcal{F}$ of polynomials $f \in \mathcal{C}_2$ with the following property: for each $f \in \mathcal{F}$, there exist arbitrarily large integers n for which $D_f(n) \notin \mathcal{Q}(f)$. Further, for any nonempty open interval $I \subseteq (2, \infty)$, there are infinitely many $f \in \mathcal{F}$ for which $\gamma(f) \in I$.

Let $\mathcal{F}$ be the set of polynomials $qX^3 + 6rX \in \mathbb{Z}[X]$ such that $q > 3$ is prime, r is not divisible by 2 or by any prime $\equiv 1 \bmod 3$, and, for $R = \prod_{p|6r} p$, we have $R < q/2$.

Lemma 19 *For $f \in \mathcal{F}$, we have $\mathcal{Q}(f) = \{kq^\ell : \ell \geq 0,\, k \mid R\}$, so $f \in \mathcal{C}_2$.*

Proof. Dickson showed long ago that the polynomial $x^3 - cx$ does not permute $\mathbb{Z}/p\mathbb{Z}$ if $p > 3$ and $p \nmid c$; see [12, Prop. 4.6] for a quick proof of this fact. It follows that the only primes in $\mathcal{Q}(f)$ are the primes dividing qR. The lemma follows easily. ∎

Lemma 20 *For $f \in \mathcal{F}$ and any $\ell \geq 0$, we have $D_f(1 + Rq^\ell) \notin \mathcal{Q}(f)$.*

Proof. Put $n = 1 + Rq^\ell$. The least element of $\mathcal{Q}(f)$ which is $\geq n$ is $q^{\ell+1}$. We will show that $D_f(n) \leq 2Rq^\ell$; since $2Rq^\ell < q^{\ell+1}$, this implies that $D_f(n) \notin \mathcal{Q}(f)$. Thus, we have only to show that $f(1), \ldots, f(n)$ are distinct modulo $2Rq^\ell$. Suppose $0 < a < b \leq n$ satisfy $f(a) \equiv f(b) \pmod{2Rq^\ell}$. First, since $0 < b - a < n < 2Rq^\ell$, we have $a \not\equiv b \pmod{2Rq^\ell}$. Since $Rq^\ell \in \mathcal{Q}$ and $f(a) \equiv f(b) \pmod{Rq^\ell}$, we must have $a \equiv b \pmod{Rq^\ell}$, so $b \geq Rq^\ell + 1$ and $a \not\equiv b \pmod 4$. This last fact, together with $f(a) \equiv f(b) \pmod 4$ and $f(X) \equiv qX^3 + 2X \pmod 4$, implies that $a \equiv b \equiv 0 \pmod 2$. Thus $b \neq Rq^\ell + 1$, so $b \geq Rq^\ell + 2 = n + 1$, a contradiction which completes the proof. ∎

These two lemmas imply the following result.

Proposition 21 *For each of the (infinitely many) polynomials $f \in \mathcal{F}$, the set $\mathcal{Q}(f)$ is infinite and yet there exist arbitrarily large integers n for which $D_f(n) \notin \mathcal{Q}(f)$.*

Define $\mathcal{N}$ to be the set of all numbers $\gamma(f)$, where f ranges over the polynomials in $\mathbb{Z}[X]$ for which $\mathcal{Q}(f)$ is infinite and yet $D_f(n) \notin \mathcal{Q}(f)$ for infinitely many n. We shall examine the subset of $\mathcal{N}$ consisting of $\gamma(f)$ for $f \in \mathcal{F}$. We will need a certain analogue of Bertrand's Postulate, due to Breusch [3].

Theorem (Breusch) *For every $m \geq 6$, there is a prime $p \equiv 2 \pmod 3$ for which $m < p < 2m$.*

Let $p_1 < p_2 < \dots$ be the odd primes congruent to 2 (mod 3). When r is the product of the first several p_i, we can describe $\gamma(f)$ precisely.

Lemma 22 *If $r = p_1 p_2 \dots p_s$, then $\gamma(f) = q/(6r)$.*

Proof. Here $R = 6r$. Let $1 = d_1 < d_2 < \cdots < d_t = R$ be the divisors of R. Since $f \in \mathcal{C}_2$, by Lemma 5 we have $\gamma(f) = \max\{q/R,\, d_{i+1}/d_i \colon 1 \leq i < t\}$. Since $q/R > 2$, it suffices to show that each $d_{i+1}/d_i \leq 2$. If $2 \nmid d_i$, then $2d_i \mid R$, so $d_{i+1} \leq 2d_i$; so assume $2 \mid d_i$. Write $p_{-1} = 2$ and $p_0 = 3$. Let j be the least index for which $p_j \nmid d_i$; thus $j \geq 0$ and $j \leq s$ (since $i < t$). Consider $d = d_i p_j / p_{j-1}$; the minimality of j implies that $d \in \mathbb{Z}$ and $d \mid R$, so $d_{i+1} \leq d$. If $j > 2$, namely if $p_{j-1} \geq 11$, then Breusch's theorem implies that $p_j < 2p_{j-1}$, so $d_{i+1} \leq d < 2d_i$. Likewise, if $j = 0$ or $j = 1$, since $3/2 < 2$ and $5/3 < 2$ we see that $d_{i+1} < 2d_i$. Thus we may assume $j = 2$, so $6 \mid d_i$ but $11 \nmid d_i$. Then $d_{i+1} \leq 11 d_i/6 < 2d_i$, and the proof is complete. ∎

Proposition 23 *$\mathcal{N}$ contains a dense subset of the interval $(2, \infty)$.*

Proof. It suffices to show that $\mathcal{N}$ intersects each nonempty subinterval (α, β) of $(2, \infty)$. Consider $f \in \mathcal{F}$, with b as in the preceding lemma. Since $\beta/\alpha > 1$, the Prime Number Theorem implies that, for any sufficiently large m, there is a prime in the interval $(m, m\beta/\alpha)$. Thus, when s is sufficiently large, there is a prime $q \in (6r\alpha, 6r\beta)$, so $\gamma(f) = q/(6r) \in (\alpha, \beta)$. ∎

Analogous to $\mathcal{N}$, one can define $\mathcal{Y}$ to be the set of all numbers $\gamma(f)$, where f ranges over the polynomials in $\mathbb{Z}[X]$ for which all but finitely many values $D_f(n)$ lie in $\mathcal{Q}(f)$. The theorems of the previous sections suggest that

$\mathcal{Y}$ contains many elements in the interval $[1, 2)$; one can show that $\mathcal{Y}$ contains 2 and 5/2 and 3, by showing every $D_f(n) \in \mathcal{Q}(f)$ for $f(X) = 2X^2 + X$ or $5X^2 - 2X$ or $3X^2 + X$ (the proofs are straightforward; also, for $3X^2 + X$ there is the single contrary value $D_f(4) = 7 \notin \mathcal{Q}(f)$). The value 5/2 is especially interesting, since in the next section we give an example showing that $5/2 \in \mathcal{N}$; thus, the value $\gamma(f)$ does not by itself determine whether $D_f(n) \in \mathcal{Q}(f)$ for all large n. Moreover, our polynomial in the next section has the same set $\mathcal{Q}(f)$ as does the polynomial $5X^2 - 2X$, so the set $\mathcal{Q}(f)$ does not by itself determine whether $D_f(n) \in \mathcal{Q}(f)$ for large n. It would be interesting to find more information about $\mathcal{N}$ and $\mathcal{Y}$. In particular, it is not clear whether $2 \in \mathcal{N}$, or whether $\mathcal{Y}$ contains arbitrarily large values.

6 Computing D_f when $\gamma(f) \geq 2$

In order to illustrate how to compute D_f when $\gamma(f) \geq 2$, we consider the example $f(X) = 5X^3 - 2X$. One can derive some preliminary properties of D_f using methods similar to those of the previous section. To this end, we have $\mathcal{Q} = \{5^\ell,\, 2 \cdot 5^\ell \colon \ell \geq 0\}$ and $\gamma = 5/2$; moreover, $D_f(n) \notin \mathcal{Q}(f)$ for infinitely many n (since $D_f(1 + 2 \cdot 5^\ell) \leq 4 \cdot 5^\ell < 5^{\ell+1}$). In this section we derive much more information about the function D_f. Our methods also apply to many other polynomials with $\gamma \geq 2$.

We need some notation to state our result. Call an integer $m > 0$ *exceptional* if there are consecutive elements q_i, q_{i+1} of $\mathcal{Q}$, with $q_i < m < q_{i+1}$, such that $f(1), ..., f(1+q_i)$ are distinct (mod m). Thus, the set of exceptional numbers contains all values of D_f outside $\mathcal{Q}$; and conversely, between any two consecutive elements of $\mathcal{Q}$, the least exceptional number will occur as a value of D_f. However, it is not clear whether every exceptional number occurs as a value of D_f.

Proposition 24 *(1) Suppose an exceptional m is divisible by some prime other than 2 and 5. Then m has the form ps, where $p \geq 97$ is a prime and $s \in \{1, 2, 4, 5, 7, 8, 10, 14\}$.*

(2) Suppose $m = 2^k 5^\ell$. Then m is exceptional if and only if the fractional part of $k \log 2 / \log 5$ lies in the interval $[\log 4 / \log 5, 1)$.

Note that, in *(2)*, the condition does not depend on ℓ, and is true for infinitely many values of k (since $\log 2 / \log 5$ is irrational, so its (positive) integer multiples are dense mod 1).

Proof. It is easy to show that, for any odd prime $p \notin \{5, 7\}$, there exist $0 < a < b < c \le p$ such that $f(a) \equiv f(b) \equiv f(c) \pmod{p}$. For instance (for $p > 7$), otherwise one could infer that many polynomials $(f(X) - f(j))/(X - j)$ have no roots in $\mathbb{Z}/p\mathbb{Z}$, which contradicts an old result on sums of Legendre symbols (see e.g. [8, Thm. 7.8.2]). For $p > 5$ we have $V_f(p) = (2p + \left(\frac{p}{3}\right))/3$ (by [12, Prop. 4.6]), so $S(f) = 5/7$ and $L(f) = 2/3$; since $\gamma(f) = 5/2$, our general results do not apply here. Also, for $r = 49$, we have $0 < 3 < 10 < 17 < r$ and $f(3) \equiv f(10) \equiv f(17) \pmod{r}$.

Suppose that m is exceptional, and also that m is divisible by some integer $r \in \{3, 49, p > 7\}$. Say $m = rs$. So there exist $0 < a < b < c \le r$ such that $f(a) \equiv f(b) \equiv f(c) \pmod{r}$. Consider

$$\mathcal{V} = \{a + rj, b + rj, c + rj : 0 \le j \le \lfloor s/3 \rfloor\};$$

the size of $\mathcal{V}$ is $3(1 + \lfloor s/3 \rfloor) > s$. But, for any $v \in \mathcal{V}$, $f(v) \equiv f(a) \pmod{r}$; since there are only s classes mod m which are $\equiv f(a) \pmod{r}$, this implies there are distinct $x, y \in \mathcal{V}$ with $f(x) \equiv f(y) \pmod{m}$. Say $x < y$. Then $0 < x < y \le r + r\lfloor s/3 \rfloor \le r + rs/3 = m/s + m/3$. Since m is exceptional, there are consecutive elements $q_i, q_{i+1} \in \mathcal{Q}$, with $q_i < m < q_{i+1}$, such that $f(1), ..., f(1 + q_i)$ are distinct modulo m. Note that q_{i+1}/q_i is either 2 or 5/2. Thus,

$$1 + q_i < y \le m/s + m/3 < q_{i+1}/s + q_{i+1}/3,$$

so $q_i/q_{i+1} < 1/s + 1/3$, i.e. $1/s > q_i/q_{i+1} - 1/3 \ge 1/15$.

There remain only the following possibilities for exceptional m:

(i) $m = 49s$, where $s \le 14$; or

(ii) $m = ps$, where $p = 3$ or $p > 7$, and $s \le 14$ (we may assume that p is the least prime dividing m, other than 2, 5, 7); or

(iii) $m = 2^k 5^\ell$; or

(iv) $m = 7 \cdot 2^k 5^\ell$.

First of all, one can check via computer that the only exceptional m less than 1250 are $4 \cdot 5^\ell$ ($\ell = 0, 1, 2, 3$) and 512. This takes care of (i). In case (ii), we must have $p \ge 1251/14 > 89$, so $p \ge 97$. Our assumption that p is the least prime dividing m, other than 2, 5, and 7, implies that s is not divisible by 3, 11, or 13, so $s \in \{1, 2, 4, 5, 7, 8, 10, 14\}$. Now we consider each of the other possibilities.

In (iii), any exceptional m will have $k \geq 2$, since we must have $m \notin \mathcal{Q}(f)$. So we assume $k \geq 2$. It is not difficult to show that $f(a) \equiv f(b) \pmod{2^k}$ if and only if either $a \equiv b \pmod{2^k}$, or both $a \equiv b \pmod{2^{k-1}}$ and a even. Thus, $f(1), f(2), ..., f(1+m/2)$ are distinct (mod m), but $f(2) \equiv f(2+m/2)$ (mod m). So m is exceptional if and only if $1 + q_i \leq m/2 + 1 \leq m < q_{i+1}$, i.e. $q_i \leq m/2 < m < q_{i+1}$. Hence $q_{i+1} > 2q_i$ whenever m is exceptional, so we must have $q_i = 2 \cdot 5^j$ and $q_{i+1} = 5^{j+1}$. Thus m is exceptional if and only if there exists $j \geq 0$ such that $2 \cdot 5^j \leq m/2 < m < 5^{j+1}$. Equivalently, $4 \cdot 5^j \leq m < 5^{j+1}$; substituting $m = 2^k 5^\ell$ gives $4 \leq 2^k 5^{\ell-j} < 5$, which can be rewritten as $\log 4/\log 5 \leq k \log 2/\log 5 + (\ell - j) < 1$. Since $k \log 2/\log 5 > 0$, this last inequality will never be satisfied with $j < 0$; thus, m is exceptional if and only if the fractional part of $k \log 2/\log 5$ lies in the interval $[\log 4/\log 5, 1)$.

Finally, we consider case (iv). Suppose $k \geq 2$, and write $m = 14z$ with $z = 2^{k-1}5^\ell$. In the following table, for z belonging to each nonzero class mod 7, we give integers $0 < a < b < m$ for which $f(a) \equiv f(b) \pmod{m}$. We make use of the fact stated in the third sentence of the previous paragraph, as well as the fact that $f(4) \equiv f(6) \pmod{7}$.

z mod 7	1	2	3	4	5	6
a	4	4	4	6	6	6
b	$4+2z$	$4+z$	$4+3z$	$6+3z$	$6+z$	$6+2z$

If m is exceptional, there are consecutive elements $q_i, q_{i+1} \in \mathcal{Q}(f)$, with $q_i < m < q_{i+1}$, such that $f(1), \ldots, f(q_i + 1)$ are distinct modulo m. This implies that $q_i < 5+3z < 14z = m < q_{i+1}$, so $2/5 \leq q_i/q_{i+1} < (5+3z)/(14z)$. It follows that $28z < 25+15z$, so $z < 25/13$ and thus $z = 1$. This contradicts our assumption that $k \geq 2$. Finally, the cases $k = 0$ and $k = 1$ can be treated in a similar manner. This completes the proof. ■

We now give some examples of *(2)*. For $k \leq 100$, this criterion implies that the number $2^k 5^\ell$ is exceptional if and only if

$$k \in \{2, 9, 16, 23, 30, 37, 44, 51, 58, 65, 74, 81, 88, 95\}.$$

We have done further work which explains the rather obvious patterns among these k's; moreover, we can show that every sufficiently large exceptional value occurs as $D_f(n)$ for some n, and that there is an upper bound on p in *(1)*. These results will be explained in a subsequent paper; the latter two results rely on estimates for the number of roots of a multivariate polynomial in a product of intervals in $(\mathbb{F}_p)^j$.

7 Generalizations

Define $D_f(a,n)$ to be the least positive integer k such that the n integers $f(a+1), f(a+2), \ldots, f(a+n)$ are distinct modulo k; thus, $D_f(0,n) = D_f(n)$. The results of this note apply to $D_f(a,n)$; in particular, in several instances they show that $D_f(a,n) = D_f(n)$ for all sufficiently large n. For, define $g(X) = f(a+X)$; then $D_f(a,n) = D_g(n)$. Since $V_f(m) = V_g(m)$ for every $m > 0$, f and g have the same $\mathcal{Q}, \gamma, S,$ and L. Thus, all the results of this paper apply to D_g whenever they apply to D_f. For instance, whenever one of these results implies that $D_f(n) \in \mathcal{Q}(f)$, it simultaneously implies that $D_g(n) \in \mathcal{Q}(f)$; moreover, $D_f(n) = D_g(n) = D_f(a,n)$.

One could also extend our results to rational functions. Here one must be careful to give the correct definitions. Let $f(X) = g(X)/h(X)$ be a rational function, where $g, h \in \mathbb{Z}[X]$ are coprime. We define $D_f(n)$ to be the least positive integer k such that both

(1) for any $a \in \mathbb{Z}$, the value $h(a)$ is coprime to k; and

(2) $f(1), f(2), \ldots, f(n)$ are distinct modulo k.

The first condition guarantees that f defines a function $\mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$. We must modify our defintions of $S(f)$, $L(f)$, and $\mathcal{Q}(f)$ by incorporating into each the hypothesis (1). When this is done, all the proofs in this paper apply at once to rational functions as well as polynomials, with one notable exception, namely the proof of Lemma 3. That proof relied on Schur's Conjecture (now Fried's Theorem), which classifies the polynomials in $\mathcal{A}$. No such classification is known for rational functions. However, one can give an alternate proof of Lemma 3 which applies to rational functions as well as polynomials. To this end, let $f \in \mathcal{A}$ be a rational function, and let Ω be the Galois closure of the field extension $\mathbb{Q}(X)/\mathbb{Q}(f(X))$. Let K be the algebraic closure of $\mathbb{Q}$ in Ω. The proof of [7, Prop. 2.1] shows that $\mathcal{Q}(f)$ contains all sufficiently large primes whose Frobenius symbol (for the extension $K/\mathbb{Q}$) lies in a certain conjugacy class of $\mathrm{Gal}(K/\mathbb{Q})$. Strong forms of the Chebotarev Density Theorem then imply that $\gamma(f) = 1$. Thus, all the results of this paper remain valid in the more general setting of rational functions.

Acknowledgement
I thank P. Moree for comments on an earlier version of this paper. He also deserves credit for introducing me to this topic; I would not have written this paper had he not sent me a preprint of [10].

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer, Note on a problem of Chowla, *Acta Arith.* **5** (1959), 417–423.

[2] P. S. Bremser, P. D. Schumer, and L. C. Washington, A note on the incongruence of consecutive integers to a fixed power, *J. Number Theory* **35** (1990), 105–108.

[3] R. Breusch, Zur verallgemeinerung des Bertrandschen postulates, dass zwischen x und $2x$ stets primzahlen liegen, *Math. Z.* **34** (1932), 505–526.

[4] S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* **17** (1970), 255–271.

[5] H. Davenport, "Multiplicative Number Theory," 2nd ed., Springer-Verlag, New York, 1980.

[6] M. Fried, On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.

[7] M. Fried, Galois groups and complex multiplication, *Trans. Amer. Math. Soc.* **235** (1978), 141–163.

[8] H. L. Keng, "Introduction to Number Theory," Springer-Verlag, New York, 1982.

[9] R. Lidl, G. L. Mullen, and G. Turnwald, "Dickson Polynomials," Pitman Monographs and Surveys in Pure and Applied Mathematics, Vol. 65, Longman Scientific, Essex, England, 1993.

[10] P. Moree, The incongruence of consecutive values of polynomials, *Finite Fields Appl.* **2** (1996), 321–335.

[11] P. Moree and G. L. Mullen, Dickson polynomial discriminators, *J. Number Theory* **59** (1996), 88–105.

[12] G. Turnwald, A new criterion for permutation polynomials, *Finite Fields Appl.* **1** (1995), 64–82.

[13] G. Turnwald, Permutation polynomials of binomial type, *in* "Contributions to General Algebra 6", pp. 281-286, Verlag Hölder-Pichler-Tempsky, Wien, 1988.

[14] D. Wan, A p-adic lifting lemma and its applications to permutation polynomials, *in* "Finite Fields, Coding Theory, and Advances in Communications and Computing," pp. 209–216, Lecture Notes in Pure and Appl. Math., Vol. 141, Dekker, New York, 1993.