POLYNOMIALS WITH NO SMALL PRIME VALUES

KEVIN S. McCURLEY

Abstract. Let \( f(x) \) be a polynomial with integer coefficients, and let
\[ D(f) = \gcd\{ f(x) : x \in \mathbb{Z} \} . \]
It was conjectured by Bouniakowsky in 1857 that if \( f(x) \) is nonconstant and irreducible over \( \mathbb{Z} \), then \( |f(x)|/D(f) \) is prime for infinitely many integers \( x \). It is shown that there exist irreducible polynomials \( f(x) \) with \( D(f) = 1 \) such that the smallest integer \( x \) for which \( |f(x)| \) is prime is large as a function of the degree of \( f \) and the size of the coefficients of \( f \).

Let \( f(x) \) be a polynomial with integer coefficients, and let \( D(f) \) be the largest integer \( D \) such that \( D \) divides \( |f(x)| \) for all integers \( x \). It was conjectured by Bouniakowsky [B] in 1857 that if \( f(x) \) is nonconstant and irreducible over the rationals, then \( |f(x)|/D(f) \) is prime for infinitely many integers \( x \). This conjecture is only known to be true in the case where \( f(x) \) is of degree one, when Bouniakowsky’s conjecture is equivalent to the well-known theorem of Dirichlet on primes in arithmetic progressions.

If Bouniakowsky’s conjecture is true, then it seems natural to ask the question: How large is the smallest integer \( x \) for which \( |f(x)|/D(f) \) is prime? In the case where \( f(x) \) is of degree one, an answer to this question is provided by a result of Linnik, that if \( (a, q) = 1 \), then the least prime congruent to \( a \) modulo \( q \) does not exceed \( q^{1/6} \). (In this note we use \( c_1, c_2, \ldots \) to denote positive absolute constants.) On the other hand, it was proved by Prachar [P] that there exist positive integers \( a \) and \( q \) with \( a < q \) and \( (a, q) = 1 \) such that \( a + qx \) is composite for all integers \( x \) with
\[ 0 < x < c_2 \log q \log_2 q \frac{\log_4 q}{(\log_3 q)^2} , \]
where \( \log_k q \) is the \( k \)-fold iterated natural logarithm. In a previous paper by the author [M] a result was proved for polynomials of higher degree that is analogous to the result of Prachar. The purpose of the present note is to prove a stronger result of this type.

In order to provide a means to measure the size of the least \( x \) for which \( |f(x)|/D(f) \) is prime, we define the length \( L(f) \) of a polynomial as follows.

Definition. If \( f(x) = \sum_{k=0}^{n} a_k x^k \) with \( a_k \in \mathbb{Z} \), then \( L(f) = \sum_{k=0}^{n} ||a_k|| \), where \( ||a_k|| \) is the number of digits in the binary expansion of \( a_k \), with \( ||0|| = 1 \).

Received by the editors March 28, 1985.
This definition is motivated by computer science concerns (see [M]), but the result of this paper could be as easily formulated in terms of some other measure of the size of \( f \), e.g. \( L^* (f) = \log (\sum_{k=0}^{n} a_k^2) \).

In [M] it was proved that there exist irreducible polynomials \( f(x) \) of arbitrarily large degree with \( D(f) = 1 \) such that \( |f(x)| \) is composite for all integers \( x \) with

\[
|x| < \exp \left( \exp \left( c_3 \frac{\log L(f)}{\log_2 L(f)} \right) \right).
\]

It was conjectured by Adleman and Odlyzko [AO] that if \( f \) is irreducible, then the least \( x \) for which \( |f(x)|/D(f) \) is prime is \( \ll \exp (L(f)^{c_4}) \). The following result shows that this conjecture is essentially best possible, since we must have \( c_4 \geq 1/2 \).

**Theorem.** There exist irreducible polynomials \( f(x) \) of arbitrary degree with \( D(f) = 1 \) such that \( |f(x)| \) is composite for all integers \( x \) with

\[
|x| < \exp \left( c_5 L(f)/\log L(f) \right).
\]

The proof of this result is constructive and extremely simple, relying only on the Prime Number Theorem.

The principle behind the proof of this result is to choose \( f(x) \) in such a way that the congruence \( f(x) \equiv 0 \pmod{p} \) has \( p - 1 \) solutions modulo \( p \) for all odd primes \( p \) with \( p - 1 \leq n = \text{degree of } f \). This forces the values of \( x \) for which \( |f(x)| \) is prime to belong to an arithmetic progression with modulus \( \prod_{3 \leq p \leq n+1} p \).

Let \( p_1 < p_2 < \cdots < p_m \) be the first \( m \) odd primes, where \( m \) is large. The following polynomials will be demonstrated to satisfy the claim made in the theorem of this note:

\[
f(x) = 2p_1 \cdots p_m + \sum_{k=1}^{m-1} 2p_{k+1} \cdots p_m \prod_{i=1}^{p_k-1} (x + 2i) + \prod_{i=1}^{p_m-1} (x + 2i).
\]

Note that \( f(x) = \sum_{k=0}^{n} a_k x^k \), where \( a_n = 1, n = \text{degree of } f, a_k \equiv 0 \pmod{2}, 0 \leq k < n. \) Furthermore we have \( a_0 \equiv 2 \pmod{4} \), so that \( f(x) \) is irreducible by Eisenstein's Criterion.

Since \( f(-2) = 2p_1 \cdots p_m \) and \( f(1) \) is odd, it follows that \( D(f) \) divides \( p_1 \cdots p_m \).

Note that if \( 1 \leq k \leq m, \) then

\[
f(x) \equiv b_k \prod_{i=1}^{p_k-1} (x + 2i) \pmod{p_k}
\]

for some integer \( b_k \) with \( b_k \not\equiv 0 \pmod{p_k} \). Hence \( f(x) \equiv 0 \pmod{p_k} \) if and only if \( x \equiv 0 \pmod{p_k} \). From this it follows that \( D(f) = 1 \). Furthermore, if \( x \) is an integer with \( 0 < |x| < p_1 \cdots p_{m-1}, \) then at least two of the primes \( p_1, \ldots, p_m \) do not divide \( x \), and it follows that \( |f(x)| \) is composite. Since \( f(0) \) is composite, we have established the fact that if \( |f(x)| \) is prime, then \( |x| \geq p_1 \cdots p_{m-1} \).

We now estimate \( L(f) \). Note that

\[
0 \leq a_i \leq f(1) < p_m! + m2^{p_m} p_m! < p_m^{2^p} p_m!.
\]
It follows from this and Stirling’s formula that

\[ L(f) \leq p_m f(1) \leq c_5 p_m \log p_m < c_6 p_m^2 \log p_m. \]

It now suffices to observe that from the Prime Number Theorem we obtain

\[ \log(p_1 \cdots p_{m-1}) > c_7 p_m > c_8 \frac{L(f)}{\log L(f)}. \]

Observe that the polynomial \( f(x) \) given here has degree \( p_m - 1 \), but in fact there exist polynomials of every degree that satisfy Theorem 1. (If degree \( n \) is desired and \( p_m \leq n < p_{m+1} - 1 \), then it suffices to replace \( (x + 2) \) by \( (x + 2)^{n-p_m+2} \) in the definition of \( f(x) \).) This improves the result of [M], where the degree \( n \) had to be chosen from a very thin set.

REFERENCES


DEPARTMENT OF MATHEMATICS, DRB 306, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CALIFORNIA 90089-1113