BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 11, Number 1, July 1984

PRIME VALUES OF POLYNOMIALS AND IRREDUCIBILITY TESTING

BY KEVIN S. McCURLEY

In 1857 Bouniakowsky [6] made a conjecture concerning prime values of polynomials that would, for instance, imply that x^2+1 is prime for infinitely many integers x. Let $f(x)$ be a polynomial with integer coefficients and define the fixed divisor of f, written $d(f)$, as the largest integer d such that d divides $f(x)$ for all integers x. Bouniakowsky conjectured that if $f(x)$ is nonconstant and irreducible over the integers, then there exist infinitely many integers x such that $f(x)/d(f)$ is a prime. An even stronger conjecture of Bateman and Horn [3, 4] would imply that if $f(x)$ is a nonconstant irreducible polynomial of degree n, with $d(f)=1$, then

$$\pi(x;f)\sim\frac{C(f)}{n}\frac{x}{\log x},\quad \text{as } x\to\infty,$$

where $\pi(x;f)$ is the number of integers m with $1\le m\le x$ for which $|f(m)|$ is prime, and

$$C(f)=\prod_p\frac{p-w(p)}{p-1},$$

where $w(p)$ is the number of solutions of the congruence $f(x)\equiv 0 \pmod p$. The only case of this conjecture that is know to be true is when $n=1$, where the conjecture is equivalent to the prime number theorem for arithmetic progressions. At present there seems to be very little hope of proving the Bouniakowsky conjecture when $n\ge 2$, much less the Bateman-Horn conjecture.

In this note we will be concerned with a related question, namely whether there exist irreducible polynomials f with $d(f)=1$ such that the smallest value of x for which $f(x)$ is prime is somehow "large". For example, Pomerance [8] has shown that there exist linear polynomials $f(x)=a+qx$ with $0<a<q$ and $d(f)=1$ such that $f(x)$ is composite for all nonnegative integers x with

$$|x|<(e^\gamma-\epsilon)\log q\log_2 q\frac{\log_4 q}{(\log_3 q)^2},$$

where $\log_m q$ is the m-fold iterated natural logarithm. The proof of this result uses a method developed by Erdös, Rankin, and Schönhage for showing that there exist large gaps between consecutive primes. The author has recently discovered that this method will also yield nontrivial results for polynomials of higher degree. For example, it can be proved that there exist positive integers

Received by the editors November 30, 1983.
1980 *Mathematics Subject Classification.* Primary 10H20, 12A20, 68C25.

a such that x^2+a is composite for all integers x with $|x| < \log a(\log\log a)^{2-\epsilon}$. Details of this and other results will be forthcoming. In this note, however, we will instead present a somewhat different approach.

For polynomials of large degree, we should probably measure the size of the smallest x for which $f(x)$ is prime in terms of the degree of f and the size of the coefficients of f. For this reason we define the length of f, written $L(f)$, of the polynomial $f(x) = \sum_{k=0}^{n} a_k x^k$ by

$$L(f) = \sum_{k=0}^{n} ||a_k||,$$

where $||a_k||$ is the length of a_k when written in binary, with $||0|| = 1$. Our main result is the following.

THEOREM. *There exist infinitely many irreducible polynomials $f(x)$ with $d(f) = 1$ such that $f(x)$ is composite for all integers x with*

$$|x| < \exp\left(\exp\left(C_1 \frac{\log L(f)}{\log\log L(f)}\right)\right),$$

where C_1 is a positive absolute constant.

The proof of this theorem uses a result due to A. Odlyzko (see [2]) which says that there exist infinitely many integers n such that n has at least

$$\exp\left(C_2 \frac{\log n}{\log\log n}\right)$$

divisors of the form $p-1$, where p is a prime. Let n be such a number, and let $p_1, \ldots, p_k$ be the odd primes for which $p_i - 1$ divides n. We now define $f(x) = x^n + D$, where $D = p_1 \cdots p_k - 1$ or $D = 3p_1 \cdots p_k - 1$, chosen so that $D \equiv 2 \pmod 4$. It follows from Eisenstein's criterion that f is irreducible and, furthermore, $f(0) \not\equiv f(1) \pmod p$, so that $d(f) = 1$. If $x \not\equiv 0 \pmod{p_i}$, then it follows from Fermat's "little" theorem that $f(x) \equiv 0 \pmod{p_i}$, so $f(x)$ is composite. Hence if $f(x)$ is prime we have $x \equiv 0 \pmod{p_1 \cdots p_k}$, and since $f(0)$ is composite, it follows that

$$|x| \geq p_1 \cdots p_k > 2^k > \exp\left(\exp\left(C_1 \frac{\log n}{\log\log n}\right)\right)$$

provided $C_1 < C_2$ and n is sufficiently large. The theorem then follows from the fact that

$$L(f) = n + ||D|| = n + O(\log D) \sim n,$$

since for n sufficiently large we have

$$\log D < \log\left(3\prod_{d|n}(d+1)\right) < \sum_{d|n} \log(3n+3) < n^{\epsilon}.$$

Note that we have actually proved slightly more than we claimed, namely that if $f(x_1)$ and $f(x_2)$ are distinct primes, then

$$|x_1 - x_2| > \exp\left(\exp\left(C_1 \frac{\log L(f)}{\log\log L(f)}\right)\right).$$

It may be of interest to consider some examples of polynomials with $d(f) = 1$ that have no small prime values. In a computer search conducted by the author among polynomials of the form $x^n + D$, the following examples were discovered:

$$f_1(x) = x^6 + 82991, \quad \text{composite for all } |x| < 7980,$$
$$f_2(x) = x^{12} + 4094, \quad \text{composite for all } |x| < 170625,$$
$$f_3(x) = x^{12} + 488669, \quad \text{composite for all } |x| < 616980.$$

Note that the smallest prime value of $f_3(x)$ has at least seventy decimal digits!

The theorem presented here has an interesting connection with a polynomial irreducibility proving algorithm proposed by Brillhart [5]. He observed that if m is an integer for which all zeros of $f(x)$ lie in $|x| < m$, and if $f(x_0)$ is prime for some integer x_0 with $|x_0| \geq m + 1$, then f is irreducible over the integers. Brillhart gave two methods for calculating m. For the polynomials constructed in the proof of our theorem, one method gives $m = D + 1$, and the other method gives $m = 2$ if n is sufficiently large. Suppose now that we test individually the numbers $f(\pm(m + k))$, $k = 1, 2, \ldots$, until we find a prime value. According to the theorem, we would have to test at least

$$\exp\left(\exp\left(C_1 \frac{\log L(f)}{\log\log L(f)}\right)\right)$$

values before we found a prime. In the language of computational complexity theory, this means that the algorithm will not terminate in polynomial time, since the number of operations required grows faster than any polynomial function of $L(f)$, the length of the input to the algorithm.

We have shown that there exist polynomials f with $d(f) = 1$ having an extremely low density of prime values, and that this can cause some difficulties in finding a prime value of f, but this does not altogether invalidate the usefulness of Brillhart's criterion. First of all, the type of behaviour exhibited by the polynomials in this note is probably quite rare, and it is probably not difficult to locate a prime value of an "average" polynomial with $d(f) = 1$. Furthermore, as Brillhart himself observed, if p divides $f(x)$, then p also divides $f(x + kp)$ for every k, and this fact can be used in a sieve procedure to remove from consideration many other values of x. This sort of approach has also been suggested by Adleman and Odlyzko [1]. They also describe how to deal with the case $d(f) \neq 1$.

In closing we note that Lenstra, Lenstra, and Lovasz [7] have recently proved that there exists a polynomial time algorithm to factor polynomials over the integers, and hence also to prove irreducibility. It remains to be seen whether there exists an algorithm to decide if f is irreducible that has a shorter running time than the known algorithms that depend on an attempt to factor f. This appears to be the case in the corresponding problem for integers (see [2]), where the current methods for primality testing are much faster than current factorization methods.

REFERENCES

1. L. M. Adleman and A. M. Odlyzko, *Irreducibility testing and factorization of polynomials*, Math. Comp. **41** (1983), 699–709.

2. L. M. Adleman, C. Pomerance and R. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983), 173–206.

3. P. T. Bateman and R. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math Comp. **16** (1962), 363–367.

4. ——, *Primes represented by irreducible polynomials in one variable*, Proc. Sympos. Pure Math., vol. 8, Amer. Math. Soc., Providence, R.I., 1965, pp. 119–135.

5. J. Brillhart, *Note on irreducibility testing*, Math. Comp. **35** (1980), 1379–1381.

6. V. Bouniakowski, *Sur les diviseurs numeriques invariables des fonctions rationelles entieres*, Mem. Acad. Sci. St. Petersburg **6** (1857), 305–329.

7. A. K. Lenstra, H. W. Lenstra and L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

8. C. Pomerance, *A note on the least prime in an arithmetic progression*, J. Number Theory **12** (1980), 218–223.

DEPARTMENT OF MATHEMATICS, MICHIGAN STATE UNIVERSITY, EAST LANSING, MICHIGAN 48824