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.

0273-0979/84 $1.00 + $.25 per page