ON THE GREATEST PRIME FACTOR OF A POLYNOMIAL

by M. KEATES

(Received 20th September 1968)

Let $f(x)$ be a non-linear polynomial with rational integer coefficients, and for integral x let $P(x)$ denote the greatest (positive) prime factor of $f(x)$. Pólya (**1**) has proved that if $f(x)$ is of degree 2 and has distinct roots then $P(x) \to \infty$ as $x \to \infty$. It is probably well-known that, provided $f(x)$ has distinct roots, this is true whatever the degree of $f(x)$. There does not appear to be a proof of this in the literature, but it is easily deducible from a result of Siegel (**2**). These results, however, are non-effective, although effective results have been obtained for a number of special polynomials. Chowla (**3**) has proved that, if $f(x) = x^2+1$, then $P(x) > C \log \log x$, where C is an absolute positive constant. Analogous results have been proved for some polynomials of the form ax^2+b and for some of the form ax^3+b by Mahler and Nagell respectively (**4**).

As a result of recent work by Baker (**5**) an effective result can now be obtained for any quadratic or cubic polynomial with distinct zeros. We first state Baker's result and then generalise it slightly. It is this generalisation which is the essential step in proving the above result in the case when $f(x)$ is a cubic.

I am indebted to Professor Hooley for pointing out this application of Baker's work.

Lemma. (Baker's Theorem). *Let $f(x)$ be a polynomial of (proper) degree* 3 *with distinct roots, and let it have rational integer coefficients with absolute value at most H. Then all solutions in integers x, y of the equation $f(x) = y^2$ satisfy*

$$\max(|x|, |y|) < \exp\{(10^6 H)^{10^6}\}. \tag{1}$$

Corollary. *Let $f(x)$ be as above and let m be a non-zero integer. Then for all integer solutions x, y of*

$$f(x) = my^2, \tag{2}$$

we have

$$|x| < \exp\{(10^7 m^2 H)^{10^6}\}. \tag{3}$$

Proof. Let x_1 be any solution of the congruence $f(x) \equiv 0 \pmod{m}$ such that $0 \leqq x_1 < |m|$. Then any solution of (2) is of the form $x = mz + x_1$, where z is a solution of

$$\frac{f(mz+x_1)}{m} = y^2.$$

The left-hand side of this last equation is a polynomial in z satisfying the conditions of the lemma, but with H replaced by $6m^2H$. Hence

$$|x| < (|m|+1) \exp\{(6 \,.\, 10^6 m^2 H)^{10^6}\} < \exp\{(10^7 m^2 H)^{10^6}\}.$$

Theorem I. *Let $f(x)$ be a quadratic or cubic polynomial with rational integer coefficients and distinct roots. Then for all x, sufficiently large in absolute value,*

$$P(x) > 10^{-7} \log\log |x|.$$

Proof. Let X be a sufficiently large constant depending on the coefficients of the polynomial, suppose throughout that $|x| > X$, and let N be the product of the primes up to and including $P(x)$.

Case 1: Quadratic Polynomials. Let $f(x) = ax^2+bx+c$ and let y^3 be the greatest cube divisor of $4af(x)$. Then $4af(x) = ny^3$, where $|n| \leqq N^2$. Hence

$$ny^3 + b^2 - 4ac = (2ax+b)^2$$

and, since $b^2 - 4ac \neq 0$, the left-hand side is a polynomial in y satisfying the conditions of the lemma with

$$H = \max(|n|, |b^2-4ac|) \leqq N^2.$$

Hence, by (1),

$$|x| < |2ax+b| < \exp\{(10^6 N^2)^{10^6}\}$$

and, since $P(x) \sim \log N$,

$$P(x) > 10^{-7} \log\log |x|.$$

Case 2: Cubic Polynomials. Let y^2 be the greatest square divisor of $f(x)$. Then $f(x) = my^2$, where $|m| \leqq N$ and, by (3),

$$|x| < \exp\{(10^7 m^2 H)^{10^6}\} < \exp\{(10^7 H \,.\, N^2)^{10^6}\}$$

and again, since $P(x) \sim \log N$,

$$P(x) > 10^{-7} \log\log |x|.$$

In a somewhat similar fashion, one can prove

Theorem II. *Let $f(x) = Ax^k + B$, where A and B are non-zero rational integers and k is an integer not less than 3. Then for all x, sufficiently large in absolute value,*

$$P(x) > (10k)^{-6} \log\log |x|.$$

The proof consists in setting $f(x) = my^k$ where y^k is the greatest k-th power divisor of $f(x)$. Then $my^k - Ax^k = B$, $|m| \leqq N^{k-1}$, and the result follows from Baker's more general result on the size of the solutions of $\phi(x, y) = B$, where ϕ is homogeneous, irreducible, and of degree at least 3. See (6).

In a paper to appear shortly Baker establishes bounds for the size of the integer solutions of the equation $f(x) = y^2$ when $f(x)$ is of degree greater than 3. This implies an effective lower bound for $P(x)$ for any non-linear polynomial with distinct roots.

REFERENCES

(1) G. Pólya, Zur arithmetischen Untersuchung der Polynome, *Math. Zeitschrift*, **1** (1918), 143-148.

(2) C. L. Siegel (extract from a letter to L. J. Mordell), The integer solutions of the equation $y^2 = ax^3+bx^2+cx+d$, *J. London Math. Soc.*, **1** (1926), 66-68.

(3) S. Chowla, The greatest prime factor of x^2+1, *J. London Math. Soc.*, **10** (1935), 117-120.

(4) K. Mahler, Uber den grössten Primteiler spezieller Polynome zweiten Grades, *Archiv for Mathem. og Natur.*, **41** (1934), No. 6.

(5) A. Baker, The Diophantine equation $y^2 = ax^3+bx^2+cx+d$, *J. London Math. Soc.*, **43** (1968), 1-9.

(6) A. Baker, Contributions to the theory of Diophantine equations, *Trans. Roy. Soc. London* Ser. A, **263** (1968), 173-208.

Department of Pure Mathematics
University College, Cardiff