ACTA ARITHMETICA
XXVI (1975)

The greatest prime factor of $a^n - b^n$

by

C. L. STEWART (Cambridge)

1. Introduction. It was conjectured by Erdös (see p. 218 of [4]) in 1965 that $P(2^n-1)/n$ tends to infinity with n, where $P(m)$ denotes the greatest prime factor of m. The elementary result that $P(a^n-b^n) \geqslant n+1$ when $n > 2$ and $a > b > 0$, was first proved by Zsigmondy [8] in 1892 and the result was rediscovered by Birkhoff and Vandiver [3] in 1904. It was improved by Schinzel [6] in 1962; he showed that $P(a^n-b^n) \geqslant 2n+1$ if ab is a square or twice a square, provided that one excludes the cases $n = 4, 6, 12$ when $a = 2$ and $b = 1$. In the present paper we shall obtain some further results in this context; in particular we shall prove that

$$P(a^n-b^n)/n \to \infty \tag{1}$$

as n runs through the sequence of primes, and, in fact, more generally, as n runs through a certain set of integers of density 1 which includes the primes.

For any integer $n > 0$ and relatively prime integers a, b with $a > b > 0$, we denote by $\Phi_n(a, b)$ the nth cyclotomic polynomial, that is

$$\Phi_n(a, b) = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (a - \zeta^i b), \tag{2}$$

where ζ is a primitive nth root of unity. We shall write, for brevity,

$$P_n = P\big(\Phi_n(a, b)\big).$$

Our main theorem is then as follows:

THEOREM 1. *For any $\varkappa$ with $0 < \varkappa < 1/\log 2$ and any integer n (> 2) with at most $\varkappa \log\log n$ distinct prime factors, we have*

$$P_n/n > f(n) \tag{3}$$

where f is a function, strictly increasing and unbounded, which can be specified explicitly in terms of a, b and $\varkappa$ only.

It will be observed that, since almost all integers n have $\big(1+o(1)\big)\times$

$\times \log\log n$ distinct prime factors (see p. 356 of [5]), the density of the set of integers covered by Theorem 1 is 1. Actually to demonstrate that $P_n/n \to \infty$ as n runs through all integers excluding a set of density zero is relatively easy; in fact it follows from [3] or [8] that $\Phi_n(a, b)$ has a prime factor of the form $kn+1$ for all $n > 6$ whence, for any f as in Theorem 1, (3) holds for every n such that $kn+1$ is composite for $k = 1, 2, \ldots, f(n)$, and, by the prime number theorem, these n have density 1 if $f(n) = o(\log n)$(¹). However, this clearly does not yield the characterisation of the integers as described in our theorem.

The size of f relative to n will be explicitly determined in the case when n is a prime or twice a prime:

THEOREM 2. *There exists an effectively computable number C, depending only on a and b, such that*

$$P_p > \tfrac{1}{2}p(\log p)^{1/4}, \qquad P_{2p} > p(\log p)^{1/4}$$

for all primes $p > C$.

The proofs of both Theorems 1 and 2 depend on the theory of Baker on linear forms in the logarithms of rational numbers; for Theorem 1 we require the most recent result of Baker [2] on the subject, while for Theorem 2 we utilize [1].

To show that Theorem 1 implies that (1) holds for all integers n as specified in the enunciation, whence, in particular, for the primes, we use the equation

$$a^n - b^n = \prod_{d|n} \Phi_d(a, b) \tag{4}$$

which follows directly from (2); this plainly gives

$$P(a^n - b^n) \geqslant P_n.$$

Similarly we deduce that

$$P\big((a^n - b^n)/(a^r - b^r)\big)/n \to \infty$$

for any factor r of n with $r \neq n$, and on replacing n by $2n$ and taking $r = n$, we see that

$$P(a^n + b^n)/n \to \infty$$

as n runs through all integers as above. Furthermore, in view of Theorem 2, we have

$$P(a^p - b^p) > \tfrac{1}{2}p(\log p)^{1/4}, \qquad P(a^p + b^p) > p(\log p)^{1/4}$$

(¹) I am grateful to Professor Erdös for pointing this out. To obtain the estimate $o(\log n)$ one should note that, by [3], the prime factors of $\Phi_n(a, b)$ specified above are distinct for different n. In fact a slightly weaker estimate follows directly from theorems on primes in arithmetic progressions.

for all sufficiently large primes p, and clearly the lower bound for these is effective.

2. Preliminaries. First we record the two results of Baker mentioned in § 1 which are required in the proofs of Theorems 1 and 2. We shall denote by $a_1, \ldots, a_n$ positive rationals and we shall suppose that, for each j, the numerator and denominator of a_j do not exceed A_j ($\geqslant 4$). Further we denote by $b_1, \ldots, b_n$ rational integers with absolute values at most B ($\geqslant 4$), and we write, for brevity,

$$\Lambda = b_1 \log a_1 + \ldots + b_n \log a_n.$$

We have

LEMMA 1. *If $\Lambda \neq 0$ then $|\Lambda| > B^{-C\Omega\log\Omega}$, where*

$$\Omega = \log A_1 \ldots \log A_n$$

and $C = C(n)$ is an effectively computable number depending only on n.

LEMMA 2. *If $\Lambda \neq 0$ then*

$$\log|\Lambda| > -\max\{\delta B, (4^{n(n+2)}\delta^{-1}\log A)^{(2n+1)^2}\}, \tag{5}$$

where $A = \max A_j$ and δ is any number satisfying $0 < \delta \leqslant 1$.

Lemma 1 is the main theorem of [2]; Lemma 2 is given by [1].

We need also a lemma on the prime decomposition of $\Phi_n = \Phi_n(a, b)$ implied by the work of Birkhoff and Vandiver [3]; the first version of this result was apparently obtained by Sylvester [7]. It is

LEMMA 3. *The prime $P(n)$ can divide Φ_n to at most the first power. All other prime factors of Φ_n are congruent to $1 \pmod n$.*

3. Proof of Theorem 1. We shall suppose throughout that n exceeds a sufficiently large number which is effectively computable in terms of a, b and $\varkappa$ only. Further we assume that n has at most $\varkappa\log\log n$ distinct prime factors, where $0 < \varkappa < 1/\log 2$. Let $d_0 = 1$ and let $d_1, \ldots, d_t$ be all the divisors of n with $\mu(n/d_r) \neq 0$, ordered according to size. Then there exists an integer s depending only on n such that

$$d_s/d_{s-1} \geqslant e^{(\log n)^{\lambda}}, \tag{6}$$

where $\lambda = 1 - \varkappa\log 2$. In fact one can take s as the smallest integer $\geqslant 1$ such that $d_s \geqslant n^{s/t}$, which exists since $d_t = n$, and then clearly $d_s \geqslant n^{1/t} d_{s-1}$; but we have

$$t \leqslant 2^{\varkappa\log\log n} = (\log n)^{\varkappa\log 2} \tag{7}$$

and (6) follows.

We proceed now to compare estimates for

$$R = \prod_{r=s}^{t} \{1-(b/a)^{d_r}\}^{\mu(n/d_r)}.$$

First we have

$$\max(R, R^{-1}) \leqslant \prod_{r=s}^{t} (1-x^{d_r})^{-1},$$

where $x = b/a$ and since, for d sufficiently large,

(8) $$(1-x^{d})^{-1} < 1+x^{d-1},$$

and, furthermore, by (6), $d_s \to \infty$ as $n \to \infty$, we see that the above product is at most

$$(1+x^{d_s-1})^{t} < 1+\sum_{l=1}^{t} (tx^{d_s-1})^{l}.$$

Since also, for n sufficiently large, $tx^{d_s-1} < \frac{1}{2}$ and, by hypothesis, $\varkappa < 1/\log 2$, we deduce from (7) that the above sum does not exceed

$$2tx^{d_s-1} < x^{d_s}\log n.$$

Hence, on recalling that $\log(1+y) < y$ for $y > 0$, we obtain

(9) $$|\log R| < (b/a)^{d_s}\log n.$$

Further we note that since $(a, b) = 1$ we have $R \neq 1$.

We now employ Lemma 1 to derive a lower bound for $|\log R|$. We shall need the following identity

(10) $$\Phi_n(a, b) = \prod_{d|n} (a^{n/d} - b^{n/d})^{\mu(d)}$$

which is easily verified from (4). From (10) we have

$$R = a^{-H}\Phi_n(a, b) \prod_{r=1}^{s-1} (a^{d_r} - b^{-d_r})^{-\mu(n/d_r)},$$

where

$$H = \sum_{r=s}^{t} d_r \mu(n/d_r).$$

The product here can be expressed as a rational number with numerator and denominator not exceeding $a^{d_1+\dots+d_{s-1}}$, and, by (7) again, this is at most $a^{d_{s-1}\log n}$. Further, we plainly have

$$|H| \leqslant \sum_{r=1}^{n} r \leqslant n^2.$$

Furthermore, by Lemma 3, we can write

(11) $$\Phi_n(a, b) = p_0 \prod_{j=1}^{k} p_j^{h_j},$$

where $p_1, \dots, p_k$ are distinct primes congruent to $1 \pmod n$, $h_1, \dots, h_k$ are positive integers and $p_0 = 1$ or $P(n)$. Clearly $p_0 \leqslant n$ and the h's do not exceed n^2. Thus on applying Lemma 1 with $n = k+3$ and with $a_1, \dots, a_n$ given respectively by $p_1, \dots, p_k, p_0, a$ and the rational number referred to above, we obtain

(12) $$|\log R| > B^{-C\Omega\log\Omega},$$

where $B = n^2$, $C = f_1(k)$ for some positive function f_1 of k only and

$$\Omega = \log p_1 \dots \log p_k \log n \log a \log(a^{d_{s-1}\log n}).$$

On combining (9) and (12) we get

$$d_s \log(a/b) - \log\log n < C\Omega\log\Omega\log B.$$

But we can assume that $p_1, \dots, p_k$ are each less than n^2, for otherwise the theorem is certainly valid, and thus

$$\Omega \leqslant 2^k (\log n)^{k+2} (\log a)^2 d_{s-1}.$$

Since $d_{s-1} < n$ and $B = n^2$, it follows that

$$d_s < f_2 (\log n)^{k+4} d_{s-1}$$

or some positive function $f_2 = f_2(a, b, k)$. This together with (6) gives

$$(\log n)^{\lambda} < f_3 \log\log n,$$

where $0 < \lambda < 1$ and $f_3 = f_3(a, b, k)$. Plainly we can assume that f_3, as a function of k, is strictly increasing and unbounded, and as such, can be extended to a function of the positive reals. Hence employing the inverse function of f_3, we conclude that $k > f(n)$ for some f as in the enunciation of the theorem. Finally we recall that, for $j \geqslant 1$, $p_j = q_j n + 1$ for some distinct $q_1, \dots, q_k$ and so (3) holds, as required.

4. Proof of Theorem 2. We shall assume that p is a prime exceeding a sufficiently large number effectively computable in terms of a and b only. We first establish the proposition for P_p; the result for P_{2p} follows similarly. The proof depends on a comparison of estimates for

$$R = a^p/(a^p - b^p).$$

Clearly $R > 1$ and, by (8),

$$\log R < (b/a)^{p-1}. \tag{13}$$

Further, by (10) we have

$$R^{-1} = a^{-p}(a-b)\Phi_p.$$

Thus, on appealing to (11) with $n = p$, we see that all the hypotheses of Lemma 2 are satisfied with $n = k+3$ and with $a_1, \ldots, a_n$ given respectively by $p_1, \ldots, p_k, p_0, a$ and $a-b$; and if p is sufficiently large, one can plainly take $A = P_p$, $B = p$. Furthermore, one can assume that $P_p < p^2$, for otherwise the theorem is certainly valid.

Arguing as at the end of the proof of Theorem 1, it clearly suffices to show that $k > \frac{1}{2}(\log p)^{1/4}$. We shall assume that this does not hold and obtain a contradiction. It is then readily verified that, on taking

$$\delta = \min\{1, \tfrac{1}{2}\log(a/b)\},$$

the second entry in the maximum on the right of (5) is at most

$$4^{4(k+4)^4}(2\delta^{-1}\log p)^{(2k+7)^2} < cp^{1/2}$$

where c is an effectively computable number depending on a and b, and here the number on the right is at most δp if p is sufficiently large. Hence we conclude from (5) that

$$\log\log R > -\delta p.$$

But, in view of the choice of δ, this contradicts (13) and the required result follows.

The asserted estimate for P_{2p} follows similarly by considering

$$R = (a^p + b^p)/a^p = a^{-p}(a+b)\Phi_{2p}.$$

In conclusion, I would like to express my gratitude to Dr. A. Baker for his generous assistance in the preparation of this paper and I would like to thank the Canada Council for their financial support while I was engaged on this research.

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers IV*, Mathematika 15 (1968), pp. 204–216.

[2] — *A sharpening of the bounds for linear forms in logarithms III*, Acta Arith. 27 (1975), pp. 247–252.

[3] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of $a^n - b^n$*, Ann. of Math. (2), 5 (1904), pp. 173–180.

[4] P. Erdös, *Some recent advances and current problems in number theory*, Lectures on Modern Mathematics, Vol. III, New York 1965, pp. 196–244.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*' 4th ed., Oxford 1960.

[6] A. Schinzel, *On primitive prime factors of $a^n - b^n$*, Proc. Cambridge Philos. Soc. 58 (1962), pp. 555–562.

[7] J. J. Sylvester, *On certain ternary cubic-form equations*, Amer. J. Math. 2 (1879), pp. 357–393.

[8] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. 3 (1892), pp. 265–284.

Received on 7. 1. 1974 (522)