PACIFIC JOURNAL OF MATHEMATICS
Vol. 54, No. 2, 1974

ON THE PRIME IDEAL DIVISORS OF $(a^n - b^n)$

EDWARD H. GROSSMAN

Let a and b denote nonzero elements of the ring of integers O_K of an algebraic number field K, such that ab^{-1} is not a root of unity and the principal ideals (a) and (b) are relatively prime.

DEFINITION 1. A prime ideal $\mathfrak{p}$ is called a *primitive prime divisor* of $(a^n - b^n)$ if $\mathfrak{p} | (a^n - b^n)$ and $\mathfrak{p} \nmid (a^k - b^k)$ for $k < n$.

DEFINITION 2. An integer n is called *exceptional for* $\{a, b\}$ if $(a^n - b^n)$ has no primitive prime divisors.

The set of integers exceptional for $\{a, b\}$ is denoted by $E(a, b)$. Using recent deep results of Baker, Schinzel [4] has proved that if $n > n_0(l)$ then $n \notin E(a, b)$, where $l = [K : Q]$ and n_0 is an effectively computable integer. In particular card $E(a, b) \leq n_0$. In this paper, using only elementary methods, upper bounds are obtained for card $\{n \in E(a, b) : n \leq x\}$ which are independent of a and b.

1. Introduction. The prime divisors of the sequence of rational integers $x_n = a^n - b^n$ have been studied by Birkhoff and Vandiver. They showed [**1**, p. 177] that if a and b are positive and relatively prime, then for $n > 6$ there is a prime p which divides $a^n - b^n$ and does not divide $a^k - b^k$ for $k < n$. Postnikova and Schinzel [**3**] have investigated analogues of this result for the ring of integers O_K of an algebraic number field K.

To fix our notation and terminology, a and b will always denote nonzero elements of O_K such that ab^{-1} is not a root of unity, and the principal ideals (a) and (b) are relatively prime. Note then that all the ideals $(a^n - b^n)$ are nonzero.

DEFINITION 1. A prime ideal $\mathfrak{p}$ is called a *primitive prime divisor of* $(a^n - b^n)$ if $\mathfrak{p}|(a^n - b^n)$ and $\mathfrak{p} \nmid (a^k - b^k)$ for $k < n$.

DEFINITION 2. An integer n is called *exceptional for* $\{a, b\}$ if $(a^n - b^n)$ has no primitive prime divisors.

The set of integers exceptional for $\{a, b\}$ is denoted by $E(a, b)$. Using a theorem of Gelfond it can be shown [**3**, p. 172] that card $(E(a, b)) < n_0(a, b)$. Recently, using deep methods, Baker [**4**] has improved Gelfond's theorem, and has shown that card $E(a, b) < n_0(l)$, where $l = [K : Q]$. In this paper we obtain by elementary methods upper bounds for card $\{n \in E(a, b) : n \leq x\}$ which are independent of a and b. To state our theorem precisely we introduce the following notation: If $M = 1$ we define $\log_1 x = \log x$ and if $M > 1$ is an integer we define $\log_M x = \log(\log_{M-1} x)$. The main result is

THEOREM 1. *Let K be a finite extension of Q of degree l, a and b elements of O_K such that $(a, b) = O_K$ and a/b is not a root of unity. If $M \geq 1$ is an integer, there is an $x_0 = x_0(M, l)$ such that for $x > x_0$,* card $\{n \in E(a, b) : n \leq x\} \leq \log_M x$.

The proof of Theorem 1 as well as related results will be found in §4. Sections 2 and 3 are preparatory.

2. Preliminary lemmas. Our first lemma provides an algebraic criterion for an integer n to be exceptional for $\{a, b\}$. Let $F_n(x, y)$ denote the nth homogeneous cyclotomic polynomial. We then have

LEMMA 1. *Let $l = [K : Q]$ and suppose $n > 2^l(2^l - 1)$. If the prime ideal $\mathfrak{p} | (a^n - b^n)$ and is not a primitive prime divisor then* $\operatorname{ord}_{\mathfrak{p}}(F_n(a, b)) \leq \operatorname{ord}_{\mathfrak{p}}(n)$. *In particular if $n \in E(a, b)$ then $(F_n(a, b)) | (n)$.*

Proof. See [3, p. 172]. We note without proof that the result also holds provided $n > 2l(2^l - 1)$.

From Lemma 1 if n is sufficiently large and $n \in E(a, b)$, then the ideal norm of $F_n(a, b)$ satisfies the inequality $N(F_n(a, b)) \leq n^l$. We will show that this can occur only if some conjugate of a/b is "very close" to a primitive nth root of unity; moreover the set of integers n for which this holds must be spaced very far apart.

We consider K as imbedded in some fixed manner in the field of complex numbers. ζ_n will denote the nth root of unity $e^{2\pi i/n}$. If a and b are any complex numbers such that a/b is not a root of unity, we let $\zeta_n^*(a, b)$ (or simply ζ_n^* if a and b are understood) denote an nth root of unity closest to a/b. For some n and complex numbers a and b, ζ_n^* is a primitive nth root of unity, for others it is not. Moreover, if there is no unique nth root of unity closest to a/b, ζ_n^* will denote a fixed nearest one. Thus

$$|a - b\zeta_n^*| = \min \{|a - b\zeta_n^{\nu}| : \nu = 1, \dots, n\}.$$

LEMMA 2. *Let $m > n$ and suppose that ζ_n^* and ζ_m^* are primitive nth and mth roots of unity satisfying*

$$|a - b\zeta_n^*| < \max(|a|, |b|) \exp(-n^{1/2})/n$$

and

$$|a - b\zeta_m^*| < \max(|a|, |b|) \exp(-m^{1/2})/m,$$

then $m \geq 2\exp(n^{1/2})$.

Proof. If $\max(|a|, |b|) = |b|$ then we have $4/mn \leq |\zeta_n^* - \zeta_m^*| \leq \exp(-n^{1/2})/n + \exp(-m^{1/2})/m \leq 2\exp(-n^{1/2})/n$ and so $m \geq 2\exp(n^{1/2})$. If $\max(|a|, |b|) = |a|$ then a similar estimate holds for $|\zeta_n^* - \zeta_m^*|$.

LEMMA 3. *Let A be a subset of the positive integers such that whenever $n, m \in A$ and $m > n$, then $m > \exp(n^{1/2})$. If M is any positive integer there is an x_M depending only on M such that for $x \geq x_M$,* $\operatorname{card}\{n \in A : n \leq x\} \leq \log_M x$.

Proof. Let $k = \operatorname{card}\{n \in A : n \leq x\}$. If $n_1 < n_2 < \cdots < n_k \leq x$ are the k elements of A less than x, then for any integer $j < k$

$$n_{k-j} \leq (3\log_j x)^2 \tag{1}$$

if $\log_j x > 2\log 3$.

We first assume $k > M + 1$. Then taking $j = M + 1$ in (1) and x large enough so that $\log_{M+1} x > 2\log 3$ we have that $n_{k-M-1} \leq (3\log_{M+1} x)^2$; in particular $k - M - 1 \leq (3\log_{M+1} x)^2$ and so $k < (M + 1) + (3\log_{M+1} x)^2$. Since this inequality also holds when $k \leq M + 1$ and $(M + 1) + (3\log_{M+1} x)^2 = o(\log_M x)$ the lemma is proven.

Denoting by $E'(a, b)$ the set of n such that ζ_n^* is a primitive nth root of unity and such that $|a - b\zeta_n^*| < \max(|a|, |b|) \exp(-n^{1/2})/n$, Theorem 1 will follow from Lemma 3 if it is shown that if n is sufficiently large and is not in $\cup E'(a^{(\nu)}, b^{(\nu)})$, where $a^{(\nu)}$ and $b^{(\nu)}$ denote the conjugates of a and b, then $n \notin E(a, b)$.

To perform the analysis we first break up $Z^+ - E'(a, b)$ into two disjoint sets:

$$S_1 = \{n : |a - b\zeta_n^*| > \max(|a|, |b|) \exp(-n^{1/2})/n\}$$

$$S_2 = \{n : |a - b\zeta_n^*| \leq \max(|a|, |b|) \exp(-n^{1/2})/n, \text{ and } \zeta_n^* \text{ not a primitive } n\text{th root of unity}\}.$$

Before continuing we note that if n is an integer for which there is no unique closest nth root of unity to a/b then $n \in S_1$.

It will be convenient to have the following notation. For any ζ_n^* let k

be the divisor of n such that ζ_n^* is a primitive kth root of unity. If $d|n$ define

$$(2)\qquad [a^d - b^d] = \begin{cases} a^d - b^d & \text{if } k\nmid d \\ \dfrac{a^d - b^d}{a - b\zeta_n^*} & \text{if } k|d. \end{cases}$$

In terms of this notation we have the following easy but basic lemma.

LEMMA 4. *If ζ_n^* is a primitive kth root of unity and $k < n$ then*

$$F_n(a,b) = \prod_{d|n} [a^d - b^d]^{\mu(n/d)}$$

Proof.

$$\prod_{d|n} [a^d - b^d]^{\mu(n/d)} = \prod_{\substack{d|n \\ k\nmid d}} (a^d - b^d)^{\mu(n/d)} \prod_{\substack{d|n \\ k|d}} \left(\frac{a^d - b^d}{a - b\zeta_n^*}\right)^{\mu(n/d)}$$

$$= F_n(a,b)(a - b\zeta_n^*)^{-L}, \quad \text{where}$$

$L = \sum_{d|n,\ k|d} \mu(n/d)$. Setting $n' = n/k > 1$, $d' = d/k$ we have $L = \sum_{d'|n'} \mu(n'/d') = 0$.

3. Bounds for $|a^d - b^d|$ and $|[a^d - b^d]|$.

The representation of $F_n(a, b)$ given in Lemma 4 as well as the usual product formula

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

will be used to provide lower bounds for $N(F_n(a, b))$. In this section we derive the necessary estimates for $|a^d - b^d|$ and $|[a^d - b^d]|$.

LEMMA 5. *For all $d \geq 1$*

$$(3)\qquad |a^d - b^d| \leq 2d \max(|a|, |b|)^d$$

$$(4)\qquad |[a^d - b^d]| \leq \begin{cases} 2d\max(|a|,|b|)^d & \text{if } k = \text{order}\, \zeta_n^* \nmid d \\ 2d\max(|a|,|b|)^{d-1} & \text{if } k = \text{order}\, \zeta_n^* | d \end{cases}$$

Proof. Inequality (3) and (4) in the case $k \nmid d$ follow from $|a^d - b^d| \leq 2\max(|a|, |b|)^d$. If $k|d$ then from (2)

$$|[a^d - b^d]| = \left|\frac{a^d - b^d}{a - b\zeta_n^*}\right| = |a^{d-1} + a^{d-2}(b\zeta_n^*) + \dots + (b\zeta_n^*)^{d-1}|$$
$$\leq d\max(|a|, |b|)^{d-1}.$$

Lower Bound Estimates: We first prove a preliminary lemma.

LEMMA 6. *Let z be a complex number such that $|z| \leq 1$ and $|z - \zeta_n^*(z, 1)| > |\zeta_n - 1| = \lambda_n$. Then $n > 6$ and $1 - |z| > (\sqrt{3}/2)\lambda_n$.*

Proof. Recall that $\zeta_n^*(z, 1)$ is a closest nth root of unity to z. First we show that if $z = re^{i\theta}$, where $1 \geq r \geq \max(0, \cos\pi/n - \sqrt{3}\sin\pi/n)$ and $|\theta| \leq \pi/n$, then $|z - 1| \leq \lambda_n$. We have in fact

$$|z - 1|^2 - \lambda_n^2 \leq (r - (\cos\pi/n - \sqrt{3}\sin\pi/n))(r - (\cos\pi/n + \sqrt{3}\sin\pi/n)) \leq 0.$$

By rotation it now follows that if $1 \geq |z| \geq \max(0, \cos\pi/n - \sqrt{3}\sin\pi/n)$ there is an nth root of unity ζ_n^v such that $|z - \zeta_n^v| \leq \lambda_n$. Finally if $n \leq 6$ we have $\cos\pi/n - \sqrt{3}\sin\pi/n \leq 0$ and so the condition $|z| \leq 1$, $|z - \zeta_n^*| > \lambda_n$ is impossible. If $n > 6$ then $1 - |z| \geq 1 - \cos\pi/n + \sqrt{3}\sin\pi/n > (\sqrt{3}/2)\lambda_n$.

LEMMA 7. *If $n \in S_1$ and $d|n$ then*

$$|a^d - b^d| \geq \max(|a|, |b|)^d \exp(-n^{1/2})/n \qquad \text{or} \tag{5}$$

$$|a^d - b^d| \geq \max(|a|, |b|)^d \left(\prod_{\zeta_d^v \neq \zeta_d^*(z,1)} |z - \zeta_d^v|\right) \exp(-n^{1/2})/n, \tag{6}$$

in which case $d > 1$ and $|z| \leq 1$ satisfies $|z - \zeta_d^*(z, 1)| \leq \lambda_d$.

Proof. Since $n \in S_1$ we can write

$$|a^d - b^d| = \max(|a|, |b|)^d |z^d - 1| \tag{7}$$

where $z = a/b$ or $z = b/a$ satisfies $|z| \leq 1$ and

$$|z - \zeta_n^*(z, 1)| > \exp(-n^{1/2})/n. \tag{8}$$

If $n \geq 1$ and $d = 1$ then (5) is immediate. If $n > 1$ and $d > 1$ we distinguish two cases accordingly as $|z - \zeta_n^*| > \lambda_n$ or $|z - \zeta_n^*| \leq \lambda_n$. In the former case Lemma 6 gives $1 - |z| > (\sqrt{3}/2)\lambda_n > 2\sqrt{3}/n$; hence $|z^d - 1| \geq 1 - |z| > 2\sqrt{3}/n > \exp(-n^{1/2})/n$, which when combined with (7) gives (5).

If $|z - \zeta_n^*| \leq \lambda_n$ then we must also have $|z - \zeta_d^*| \leq \lambda_d$. Otherwise Lemma 6 gives $(\sqrt{3}/2)\lambda_d < 1 - |z| \leq |z - \zeta_n^*| \leq \lambda_n$ which is impossible since $n/d \geq 2$. Observing now that (6) follows immediately from (7) and (8), the proof is complete.

LEMMA 8. *If $n \in S_2$ and $d|n$, then if* order $\zeta_n^* = k \nmid d$

$$|[a^d - b^d]| \geq \max(|a|, |b|)^d \exp(-n^{1/2})/n \qquad \textit{or} \tag{9}$$

$$|[a^d - b^d]| \geq \max(|a|,|b|)^d \Bigg(\prod_{\zeta_d^\nu \neq \zeta_d^*(z,1)} |z - \zeta_d^\nu| \Bigg) \exp(-n^{1/2})/n \tag{10}$$

in which case $d > 1$ and $|z| \leq 1$ satisfies $|z - \zeta_d^*| \leq \lambda_d$. If order $\zeta_n^* = k|d$

$$|[a^d - b^d]| \geq \max(|a|,|b|)^{d-1} \prod_{\zeta_d^\nu \neq \zeta_d^*} |z - \zeta_d^\nu|, \tag{11}$$

where for $d = 1$ the product on the right side of (11) is one and if $d > 1$, $|z| \leq 1$ satisfies $|z - \zeta_d^*| \leq \lambda_d$.

Proof. Since $n \in S_2$, with $z = a/b$ or b/a we have $|z| \leq 1$,

$$|z - \zeta_n^*| \leq \exp(-n^{1/2})/n \tag{12}$$

and order $\zeta_n^* = k < n$.

If $k \nmid d$ we have $n > 1$ and since ζ_n^* is not a dth root of unity (12) implies

$$|z - \zeta_d^*| \geq |\zeta_d^* - \zeta_n^*| - |z - \zeta_n^*| > \exp(-n^{1/2})/n.$$

We can now argue as in the previous lemma.

If $k|d$ then we have

$$|[a^d - b^d]| = \max(|a|,|b|)^{d-1} \left| \frac{z^d - 1}{z - \zeta_n^*(z,1)} \right| \tag{13}$$

where $|z| \leq 1$ satisfies (12). If $d = 1$ then since $k|d$, $\zeta_n^* = 1$ and (13) is precisely (11). For $d > 1$, (11) and the condition $|z - \zeta_d^\nu| \leq \lambda_d$ follow from (12) and (13) in view of $\zeta_n^* = \zeta_d^*$.

In order to complete the lower bound estimates we must obtain lower bounds for $\prod_{\zeta_d^\nu \neq \zeta_d^*} |z - \zeta_d^\nu|$, where $d > 1$ and $|z| \leq 1$ satisfies $|z - \zeta_d^*| \leq \lambda_d$. We first prove

LEMMA 9. *Let $d > 1$ be an integer and r a real number satisfying $0 \leq r \leq 1$ and $|r - 1| \leq \lambda_d$, then*

$$(14) \qquad \prod_{\nu=1}^{d-1} |r - \zeta_d^\nu| \geq d^{-3\tau+1}$$

where $\tau = \tau_d = [\sqrt{\pi d/2}] + 1$.

Proof. Since r is real we have

$$(15) \qquad \prod_{\nu=1}^{d-1} |r - \zeta_d^\nu| \geq (1/2) \prod_{\nu=1}^{[d/2]} |r - \zeta_d^\nu|^2.$$

We give a lower bound for the latter product. From $|r - 1| \leq \lambda_d$ we obtain

$$(16) \qquad |r - \zeta_d^\nu| \geq |1 - \zeta_d^\nu| - |1 - r| \geq |1 - \zeta_d^\nu| - \lambda_d.$$

Let $\tau = \tau_d = [\sqrt{\pi d/2}] + 1$ and suppose first that $[d/2] > \tau_d$ and ν satisfies $[d/2] \geq \nu > \tau_d$. Then

$$(17) \qquad |1 - \zeta_d^\nu| - |\zeta_d^\nu - \zeta_d^\tau| = 4 \sin(\pi\tau/2d) \cos \pi(\nu/d - \tau/2d)$$
$$\geq (4\tau/d)(d - 2\nu + \tau)/d \geq 4\tau^2/d^2 \geq 2\pi/d \geq \lambda_d.$$

Thus from (16), $|r - \zeta_d^\nu| \geq |\zeta_d^{\nu-\tau} - 1|$ and so

$$(18) \qquad \prod_{\nu=1}^{[d/2]} |r - \zeta_d^\nu| \geq \prod_{\nu=1}^{\tau} |r - \zeta_d^\nu| \prod_{\nu=\tau+1}^{[d/2]} |1 - \zeta_d^{\nu-\tau}|$$

$$= \frac{\prod_{\nu=1}^{\tau} |r - \zeta_d^\nu| \prod_{\nu=1}^{[d/2]} |1 - \zeta_d^\nu|}{\prod_{\nu=[d/2]-\tau+1}^{[d/2]} |1 - \zeta_d^\nu|}.$$

Since $r \geq 0$ we have

$$|r - \zeta_d^{\nu}| \geq |r - \zeta_d| > 2/d \tag{19}$$

if $d \geq 4$ and the same inequality ($|r - \zeta_d^{\nu}| \geq 2/d$) holds for $d < 4$. Observing finally that $|1 - \zeta_d^{\nu}| \leq 2$ and

$$\prod_{\nu=1}^{[d/2]} |1 - \zeta_d^{\nu}|^2 \geq \prod_{\nu=1}^{d-1} |1 - \zeta_d^{\nu}| = d$$

we obtain (14) from (15) and (18).

Now if $\tau_d \geq [d/2]$ we have from (19)

$$\prod_{\nu=1}^{d-1} |r - \zeta_d^{\nu}| \geq (2/d)^{d-1} \geq (2/d)^{2[d/2]} \geq d^{-2\tau}2^{2\tau} \geq d^{-3\tau+1}$$

and so (14) is also proven in this case.

LEMMA 10. *If $d > 1$ and $|z| \leq 1$ satisfies $|z - \zeta_d^*| \leq \lambda_d$ then*

$$\prod_{\zeta_d^{\nu} \neq \zeta_d^*} |z - \zeta_d^{\nu}| \geq d^{-3\tau} \tag{20}$$

where $\tau = \tau_d = [\sqrt{\pi d/2}] + 1$.

Proof. We may assume that $\zeta_d^* = 1$ and $z = re^{i\theta}$, where $0 \leq \theta \leq \pi/d$; thus we must prove the lower bound (20) for $\prod_{\nu=1}^{d-1} |z - \zeta_d^{\nu}|$. Let $z' = re^{2\pi i/d}$. Then if $1 \leq \nu \leq [d/2]$, $|z - \zeta_d^{\nu}| > |z' - \zeta_d^{\nu}|$ and if $[d/2] < \nu \leq d - 1$, $|z - \zeta_d^{\nu}| \geq |r - \zeta_d^{\nu}|$. Combining these results and using $|z - \zeta_d| \geq \lambda_d/2 \geq 2/d$ we obtain

$$\begin{aligned} \prod_{\nu=1}^{d-1} |z - \zeta_d^{\nu}| &\geq \frac{|z - \zeta_d|}{|r - \zeta_d^{[d/2]}|} \prod_{\nu=1}^{d-1} |r - \zeta_d^{\nu}| \\ &\geq d^{-1} \prod_{\nu=1}^{d-1} |r - \zeta_d^{\nu}|. \end{aligned} \tag{21}$$

Since $|r - 1| \leq |z - 1| \leq \lambda_d$, (20) follows from Lemma 9 and (21).

From Lemmas 7, 8 and 10 we arrive at our final lower bound estimates.

LEMMA 11. *If $n \in S_1$ and $d|n$ then*

(22) $$|a^d - b^d| \geq \max(|a|,|b|)^d d^{-3\tau}\exp(-n^{1/2})/n$$

where $\tau = \tau_d = [\sqrt{\pi d/2}] + 1$.
If $n \in S_2$, $d|n$, *then if* order $\zeta_n^*(a, b) = k \nmid d$, (22) *holds for* $|[a^d - b^d]|$. *If* $k|d$ *we have*

(23) $$|[a^d - b^d]| \geq \max(|a|, |b|)^{d-1} d^{-3\tau}.$$

4. Main theorem and related results. The proof of Theorem 1 will follow easily from the following lemma.

LEMMA 12. *There is an integer* n'_0 *such that if* $n > n'_0$ *and* $n \in S_1 \cup S_2$ *then*

(24) $$\log|F_n(a,b)| \geq \varphi(n)\max(\log|a|,\log|b|) - 2^{\nu(n)}n^{5/8}.$$

Proof. If $n \in S_1$ we use Lemmas 5 and 11 and the formula $F_n(a, b) = \prod_{d|n}(a^d - b^d)^{\mu(n/d)}$ to obtain (24).

If $n \in S_2$ then (24) follows from Lemma 4 and the estimates of Lemmas 5 and 11.

Proof of Theorem 1. Recall that $S_1 \cup S_2$ is the complement of the set $E'(a, b) = \{n \in Z^+ : |a - b\zeta_n^*| \leq \max(|a|, |b|)\exp(-n^{1/2})/n$ and ζ_n^* a primitive nth root of unity$\}$. Let $E' = \cup_{\nu=1}^{l} E'(a^{(\nu)}, b^{(\nu)})$, where $l = [K : Q]$ and $a^{(\nu)}$, $b^{(\nu)}$ denote the conjugates of a and b. If $n \notin E'$ then the lower bound (24) is valid for all ν provided $n > n'_0$. Thus

(25) $$\log|N(F_n(a,b))| = \sum_{\nu=1}^{l}\log|F_n(a^{(\nu)},b^{(\nu)})| \geq A\varphi(n) - l2^{\nu(n)}n^{5/8} \qquad \text{where}$$

(26) $$A = \sum_{\nu=1}^{l}\max(\log|a^{(\nu)}|,\log|b^{(\nu)}|) = \log|N(b)| + \sum_{\nu=1}^{l}\max\left(\log\left|\frac{a^{(\nu)}}{b^{(\nu)}}\right|, 0\right).$$

If $|N(b)| = 1$, then a/b is in O_K and there is a constant c_K, depending only on $[K : Q]$, such that $|a^{(\nu)}/b^{(\nu)}| > c_K$ for some ν. Thus $A \geq \min(\log 2,$

$\log c_K) = C'_K$. Using the well-known [2, p. 114] estimates $\varphi(n) > c_1 n/\log\log n$ and $2^{\nu(n)} < c_2(\epsilon)n^\epsilon$ (with $\epsilon = 1/8$), (25) gives

$$\log|N(F_n(a,b))| \geq \frac{C_K n}{\log\log n} - c_2 l n^{3/4} > l\log n \text{ for}$$

$n > n_0(l)$ and so from Lemma 1, $n \notin E(a, b)$.

Thus $E(a, b) \subset E' \cup \{n \leq n_0\}$ and the density estimate for $E(a, b)$ follows in view of Lemmas 2 and 3.

We can extract additional quantitative information from the above proof. Let us write $(a^n - b^n) = \mathfrak{A}\mathfrak{B}$ where $\mathfrak{A} + \mathfrak{B} = O_K$ and $\mathfrak{P}|\mathfrak{A}$ if and only if $\mathfrak{P}$ is a primitive prime divisor of $(a^n - b^n)$. We call $\mathfrak{A}$ the *primitive part* of $(a^n - b^n)$ and denote it by $P_n(a, b)$. Then we have

LEMMA 13. *If $n > n_0(K)$ and $n \notin E'$ then*

$$\log|N(P_n(a,b))| = A\varphi(n) + O(n^{3/4}) \tag{27}$$

where A is defined by (26) *and the constant implied by O depends only on K.*

Proof. Lemma 1 implies that for $n > 2^l(2^l - 1)$

$$\log|N(F_n(a,b))| - l\log n \leq \log|N(P_n(a,b))| \leq \log|N(F_n(a,b))|.$$

If $n \in S_1 \cup S_2$ the left side can be bounded from below using (24). Moreover, as in Lemma 12 one shows that for n sufficiently large, $n \in S_1 \cup S_2$

$$\log|F_n(a,b)| \leq \varphi(n)\max(\log|a|, \log|b|) + 2^{\nu(n)}n^{5/8}.$$

Using these estimates we immediately obtain (27).

Lemma 13 and the density estimate for E' enable us to derive both a normal order and average order for $\log|N(P_n(a, b))|$. The proofs are straightforward and are omitted.

THEOREM 2. *$\log|N(P_n(a, b))|$ has $\varphi(n)A$ as a normal order, i.e. for any $\epsilon > 0$ if*

$$T(\varepsilon, x) = \{n \leq x : |\log|N(P_n(a,b))| - \varphi(n)A| < \varepsilon\varphi(n)A\},$$

then card $T(\epsilon, x)/x \to 1$ *as* $x \to \infty$.

THEOREM 3. $$\sum_{n \le x} \log |N(P_n(a,b))| = \frac{3A}{\pi^2} x^2 + O(Ax^{7/4})$$

where the constant implied by $O(\ )$ *depends only on K.*

REFERENCES

1. G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. of Math., **5** (1902–03), 173–180.
2. W. J. LeVeque, *Topics in Number Theory,* vol. 1, Addison Wesley, Reading, Mass., 1956.
3. L. P. Postnikova and A. Schinzel, *Primitive divisors of the expression* $a^n - b^n$ *in algebraic number fields,* Math. U.S.S.R.-Sbornik, **4** (1968), No. 2, 153–159.
4 A. Schinzel, *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields,* J. Reine Angew. Math., **268/269** (1974), 27–33.

Received July 23, 1973.

CITY COLLEGE OF CUNY