ACTA ARITHMETICA
LXXXVI.2 (1998)

Growth of the product $\prod_{j=1}^{n}(1-x^{a_j})$

by

J. P. Bell (Waterloo, Ont.), P. B. Borwein (Burnaby, B.C.)
and L. B. Richmond (Waterloo, Ont.)

We estimate the maximum of $\prod_{j=1}^{n}|1-x^{a_j}|$ on the unit circle where $1 \le a_1 \le a_2 \le \ldots$ is a sequence of integers. We show that when a_j is j^k or when a_j is a quadratic in j that takes on positive integer values, the maximum grows as $\exp(cn)$, where c is a positive constant. This complements results of Sudler and Wright that show exponential growth when a_j is j.

In contrast we show, under fairly general conditions, that the maximum is less than $2^n/n^r$, where r is an arbitrary positive number. One consequence is that the number of partitions of m with an even number of parts chosen from $a_1, \ldots, a_n$ is asymptotically equal to the number of such partitions with an odd number of parts when a_i satisfies these general conditions.

1. Introduction. Let $A = \{a_m\}_{m=1}^{\infty}$, $a_1 < a_2 < \ldots$, denote a sequence of positive integers. Let $q^{\mathrm{e}}_{A,n}(m)$ denote the number of solutions to

$$m = a_{j_1} + \ldots + a_{j_r} \quad (1 \le j_1 < \ldots < j_r \le n)$$

where r is an even natural number and let $q^{\mathrm{o}}_{A,n}(n)$ denote the number of such solutions with r odd. We consider the generating function for $\overline{q}_{A,n}(m) \equiv q^{\mathrm{e}}_{A,n}(m) - q^{\mathrm{o}}_{A,n}(m)$:

$$F_{A,n}(x) = \prod_{j=1}^{n}(1-x^{a_j}) = \sum_{m\ge 0} \overline{q}_{A,n}(m)x^m.$$

The case of $a_j = j$ has received a very careful analysis by Sudler [16] and Wright [17], [18]. Sudler shows that if $a_j = j$ and

$$M_{A,n} = \max_m |\overline{q}_{A,n}(m)|$$

then

$$\log M_{A,n} = Kn + O(\log n)$$

1991 *Mathematics Subject Classification*: 11P76, 11C08.

where K is explicitly given ($K = .19861\ldots$). The fact that M_n grows exponentially is perhaps surprising since Euler's pentagonal number theorem states that

$$\prod_{k=1}^{\infty}(1-x^k) = \sum_{m=-\infty}^{\infty}(-1)^m x^{(3m^2+m)/2}$$

(see Hardy and Wright [9]).

Let A_p denote the sequence formed by taking the integers not divisible by the prime p. P. Borwein [3] has determined the corresponding K for the sequences A_p for $p = 3, 5, \ldots, 17$.

In this note we first derive upper bounds on $M_{A,n}$ (see Theorem 2.1) under the general conditions of Roth and Szekeres [14]. We then derive asymptotic estimates for $q^{\mathrm{o}}_{A,n}(m) \sim q^{\mathrm{e}}_{A,n}(m)$ for m sufficiently near the maximum of $q^{\mathrm{o}}_{A,n}(m)$ (see Theorem 2.2).

We next consider lower bounds for $M_{A,n}$. There is a close analogy between this problem and the following problem of Erdős and Szekeres [8]: Estimate $M(n)$ where

$$M(n) = \min_{\{k_1,\ldots,k_n\}} \max_{|x|=1} \prod_{j=1}^{n} |1 - x^{k_j}|.$$

Here $k_1, \ldots, k_n$ may be any positive integers, not necessarily the first terms of a given sequence A.

The best upper bound for $M(n)$ is that of Belov and Konyagin [2]

$$M(n) \le \exp(O((\log n)^4)).$$

Previously Atkinson [1] and Dobrowolski [6] proved the upper bound of $\exp(O(n^{1/2}\log n))$, and the upper bound of $\exp(O(n^{1/3}(\log n)^{4/3}))$ was obtained by Odlyzko [12]. M. N. Kolountzakis [10] proved the upper bound $\exp(O(n^{1/3}\log n))$ for $M(n)$.

The strongest lower bound $\sqrt{2n}$ is due to Erdős and Szekeres [8]. Erdős [7] has conjectured that for all large n, $M(n) \ge n^k$, k any constant. There has been little progress on this old conjecture. The only non-trivial results are due to Maltby [11]. These concern the norm of products of length n for $n = 7, 9, 10, 11$ and show that the L_1 norm of these products exceeds $2n$.

Define

$$\|h(x)\|_\infty = \max_{|x|=1} |h(x)|.$$

Clearly, any lower bound for $M(n)$ is a lower bound for $\|F_{A,n}(x)\|_\infty$.

We exhibit families of polynomials, $p(j)$, such that if $a_j = p(j)$ then $M_{A,n} \ge c^n$, c a positive constant. We also exhibit sequences A such that $M_{A,n} \le \exp(O(n^{1/2}\log n))$.

We further conjecture that $M_{A,n}$ grows exponentially if a_j is a polynomial that takes integral values for integral j. (Such a polynomial $p(j)$ is an integral combination of binomial coefficients.)

2. Theorems and proofs. We shall use the following two conditions of Roth and Szekeres [14] on a sequence $A = \{a_k\}$:

(I) $\lim_{k\to\infty} \log a_k/\log k = s$ exists, $s > 0$.

(II) If

$$J_k = \inf_{(2a_k)^{-1}\le\alpha\le 1/2} \frac{1}{\log k}\sum_{i=1}^{k} \|\alpha a_i\|^2,$$

then $J_k \to \infty$ as $k \to \infty$ (here $\|x\|$ denotes the distance of x from the nearest integer).

Roth and Szekeres [14] showed that the following sequences satisfy (I) and (II):

(i) The sequence $a_j = f(j)$, where $f(x)$ is a polynomial which only takes integral values for integral x and has the property that corresponding to every p there exists an integer x such that $p \nmid f(x)$.

(ii) The sequence $a_j = f(p_j)$, where $f(x)$ is a polynomial as in (i) and p_j denotes that jth prime.

Note that (ii) includes the case $a_j = p_j$. Also note that each of the above $f(x)$ is an integral combination of binomial coefficients $\binom{x}{k}$.

Theorem 2.1. *Suppose A is a non-decreasing sequence of positive integers in which infinitely many members are even, and infinitely many members are odd. Let $A_{\mathrm{o}} = \{a_{j_k}\}_{k=1}^{\infty}, a_{k_1} < a_{k_2} < \ldots$, be the subsequence of A formed by all the odd elements. Moreover, suppose that A and A_{o} satisfy* (I) *and* (II) *above. Then*

$$\|F_{A,n}(x)\|_\infty \le 2^n n^{-r} \quad \textit{for any constant } r > 0.$$

In [8] Erdős and Szekeres show that $\|F_{A,n}(x)\|_\infty = o(2^n)$ for a certain A. Theorem 2.1 shows that this is true for a quite general class of A.

Proof (of Theorem 2.1). We suppose that $\log a_j \sim t\log j$ and $\log a_{j_k} \sim s\log k$, where s and t are positive constants. Now notice that if $x = \exp(\pi i + 2\pi i\theta)$, $-1/2 \le \theta \le 1/2$ and $a_j \in A_{\mathrm{o}}$ then

$$|1 - x^{a_j}| = |1 + e^{2\pi i a_j\theta}| = 2|\cos(2\pi a_j\theta)| \le 2\exp(-c\|a_j\theta\|^2).$$

Letting a dash indicate a product over elements of A_{o}, we combine (I) and (II) to obtain

$$\Big|\prod_{j\le m}{}'(1 - x^{a_j})\Big| \le 2^{m_1} m_1^{-r} \quad \text{for each } r > 0,\ m_1 = \text{the number of factors},$$

provided $|\theta| \geq (2a_m)^{-1}$. Thus if

$$M_1 = M_1(n) = |\{a_j \mid 1 \leq j \leq n,\ a_j \in A - A_{\mathrm{o}}\}|,$$

we have

$$\|F_{A,n}(x)\|_\infty \leq 2^{n-M_1}(n-M_1)^{-r}2^{M_1} \quad \text{for all } r > 0.$$

Since $n - M_1 = |\{a_j \mid a_j \in A_{\mathrm{o}},\ a_j \leq a_n\}|$, and since A and A_{o} satisfy (I) we have $n - M_1 \geq a_n^{(1-\varepsilon)/s} \geq n^{(1-\varepsilon)/(st)}$ for $|\theta| \geq 2/a_m$, and

$$\|F_{A,n}(x)\| \leq 2^n n^{-r} \quad \text{for each } r > 0.$$

Suppose now $|\theta| \leq 2/a_m$. If $a_j \in A - A_{\mathrm{o}}$ then

$$|1 - x^{a_j\theta}| \leq ca_j/a_m.$$

Thus if $A_{\mathrm{e}} = \{a_j \mid a_j \in A - A_{\mathrm{o}},\ a_j \leq a_m^{1/2}\}$ and $M_2 = |A_{\mathrm{e}}|$ then

$$\Big|\prod_{j=1}^{n}(1 - x^{a_j\theta})\Big| \leq \Big(\prod_{a_j \in A_{\mathrm{e}}} a_l\Big)\Big(\frac{c}{a_m}\Big)^{M_2} 2^{n-M_2}$$

and since $a_m \geq n^{(1-\varepsilon)/s}$ we again have if $M_1(n) \to \infty$ as $n \to \infty$

$$\Big|\prod_{j=1}^{n}(1 - x^{a_j})\Big| \leq 2^n n^{-r} \quad \text{for each } r > 0,$$

proving Theorem 2.1.

Now Odlyzko and Richmond [13] prove

THEOREM 2.2. *Suppose A satisfies* (I) *and* (II) *above. Let*

$$N = \sum_{j=1}^{n} a_j, \qquad B = \sum_{j=1}^{n} a_j^2.$$

Let $L > 0$ be any constant. Then if $|m - N/2| \leq L\sqrt{B\log n}$ and

$$\prod_{j=1}^{n}(1 + x^{a_j}) = \sum_{m \geq 1} q_{A,n}(m)x^m$$

we have

$$q_{A,n}(m) \sim \frac{2^m\sqrt{2}}{\sqrt{\pi B}} e^{-2(m-N/2)^2/B}.$$

Theorems 2.1 and 2.2 give

THEOREM 2.3. *Suppose A satisfies* (I) *and* (II) *above. Suppose also that $A^{\mathrm{o}} = \{a_j \mid a_j \equiv 1 \pmod 2\}$ satisfies* (I) *and* (II) *above and $A - A^{\mathrm{o}}$ is infinite. With N and B defined in Theorem 2.2 and*

$$\Big|m - \frac{N}{2}\Big| \leq \sqrt{B\log n},$$

one has

$$q^{\mathrm{e}}_{A,n}(m) = q^{\mathrm{o}}_{A,n}(m)(1+O(n^{-M})) \quad \textit{for any } r>0.$$

Proof. Since $\|F_{A,n}(x)\|_\infty \le 2^n n^{-r}$ from Theorem 2.1 it follows from Cauchy's integral formula with $|x|=1$ that

$$|q^{\mathrm{e}}_{A,n}(m) - q^{\mathrm{o}}_{A,n}(m)| \le 2^n n^{-r}$$

for all $r>0$. Theorem 2.3 follows immediately from this and Theorem 2.2 for $|m-N/2| \le B^{1/2}(\log m)^{1/2}$ since

$$q^{\mathrm{e}}_{A,n}(m) + q^{\mathrm{o}}_{A,n}(m) = q_{A,n}(m).$$

We now give an example to show that we cannot in general expect exponential growth of $\|F_{n,k}(x)\|_\infty$. This is in Borwein and Ingalls [4] but it is very simple and we reproduce some of it here.

Lemma 2.1. *Let* $1 \le \beta_1 \le \beta_2 \le \ldots$ *and let*

$$W_n(z) = \prod_{1\le i<j\le n}(1-z^{\beta_j-\beta_i}).$$

Then

$$\|W_n(z)\|_\infty = \max_{|z|=1}|W_n(z)| \le n^{n/2}.$$

Proof. We explicitly evaluate the Vandermonde determinant

$$D_n(z) = \prod_{1\le i<j\le n}|z^{\beta_j}-z^{\beta_i}| = \begin{vmatrix} 1 & z^{\beta_1} & \ldots & z^{(n-1)\beta_1} \\ \vdots & \vdots & & \vdots \\ 1 & z^{\beta_n} & \ldots & z^{(n-1)\beta_n} \end{vmatrix}.$$

As each entry of the matrix has modulus ≤ 1 in the unit disc, by Hadamard's inequality, we have $\|D(z)\|_\infty \le n^{n/2}$. Thus

$$\Big\|\prod_{1\le i<j\le n}(1-z^{\beta_j-\beta_i})\Big\|_\infty = \|D_n(z)\|_\infty \le n^{n/2}.$$

Observe, as Dobrowolski did in [6], that if we take $\beta_i = i$ we have

$$\Big\|\prod_{i=1}^{n-1}(1-z^i)^{n-i}\Big\|_\infty \le n^{n/2},$$

a result first proved by Atkinson [1] using Fourier series.

Theorem 2.4. *Let* $A = \{\beta_j\}_{j=1}^{\infty}$ *be the sequence formed by taking the set* $\{2^n - 2^m \mid n > m \ge 0\}$ *in increasing order. Then for all* n:

$$\|F_{A,n}(x)\|_\infty \le (32n)^{\sqrt{n/8}}.$$

Clearly, any $\alpha \ge 2$ could play the role of 2 in the construction of the β_i's with the same conclusion. Indeed, we have

THEOREM 2.5. *Let $\{\delta_i\}$ be any sequence of integers and let $\{\beta_i\}$ be the sequences of differences in the following order*:

$$\{\delta_1-\delta_0,\delta_2-\delta_1,\delta_2-\delta_0,\ldots,\delta_n-\delta_{n-1},\ldots,\delta_n-\delta_0,\ldots\}.$$

(*So the nth block is $\{\delta_n-\delta_{n-1},\ldots,\delta_n-\delta_1,\delta_n-\delta_0\}$.*) *Then*

$$\Big\|\prod_{i=1}^{n}(1-z^{\beta_i})\Big\|_\infty \le (32n)^{\sqrt{n/8}}.$$

We now turn to the study of lower bounds for $\|F_{A,n}(x)\|_\infty$.

Let $A=\{a_j\}_{j=1}^\infty$ be a sequence of positive integers. For p a prime let $I_{n,p}=I_{A,n,p}$ be defined by

$$I_{n,p}=\{a_j\mid p\,|\,a_j,\ 1\le j\le n\}.$$

LEMMA 2.2 (Szekely). *Let $A=\{a_j\}_{j=1}^\infty$ be a sequence of positive integers. For $1\le\alpha\le p-1$, let*

$$G(\alpha,p)=\prod_{a_j\notin I_{n,p}}(1-e^{2\pi a_j\alpha/p}).$$

Define $n_0=|I_{n,p}|$. Then there is an α such that

$$|G(\alpha,p)|\ge p^{(n-n_0)/(p-1)}.$$

Proof. Note that

$$\begin{aligned}\max_{1\le a\le p-1}|G(\alpha,p)| &\ge \frac{1}{p}\sum_{\alpha=1}^{p-1}\prod_{a_j\notin I_{n,p}}|1-e^{2\pi i a_j\alpha/p}|\\ &\ge \prod_{\alpha=1}^{p-1}\prod_{a_j\notin I_{n,p}}|1-e^{2\pi i a_j\alpha/p}|^{1/(p-1)}\\ &= \prod_{a_j\notin I_{n,p}}\prod_{m=1}^{p-1}|1-e^{2\pi i m/p}|^{1/(p-1)}.\end{aligned}$$

Since the inside product is

$$\left|\lim_{x\to1}\left(\frac{1-x^p}{1-x}\right)\right|=p$$

the lemma follows.

We now give a demonstration of the fact that given a positive integer k, the maximum value of the product $\prod_{j=1}^{m}|1-x^{j^k}|$, as x takes on values on the unit circle, grows at an exponential rate with respect to m, as m grows large. From this fact, it follows in a straightforward manner that the maximal coefficient of this product (when considered as a polynomial in x) grows at an exponential rate with respect to m. It is known that the product being considered grows at an exponential rate with respect to m, when $k=1$ (see Sudler [16] and Wright [17], [18]). Thus we will restrict our attention to the case when k is an integer that is at least two. In order to obtain the desired results, we will have to appeal to some results from basic group theory and introduce some notation as well.

First, note that if k is an integer that is greater than or equal to 2, and p is a prime with $p \equiv 1 \pmod{k}$, then the set $\{j^k + p\mathbb{Z} \mid 0 < j < p\}$ forms a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ of index k. We denote this group by R_k, as it is the subgroup of kth power residues. Note that if $\phi : (\mathbb{Z}/p\mathbb{Z})^* \mapsto R_k$, is given by the assignment $j + p\mathbb{Z} \mapsto j^k + p\mathbb{Z}$, then ϕ is a group homomorphism, and hence $\mathrm{Card}(\phi^{-1}(\{j^k + p\mathbb{Z}\})) = k$. Also note that if $(p-1)/k$ is even, then $-1+p\mathbb{Z}$ is an element of R_k. We now proceed to prove the result mentioned earlier.

LEMMA 2.3. *Suppose* $k \in \mathbb{N}$, *and* $p = 1 + 2kM$ *is prime. Then there is an integer* q *such that*

$$\prod_{s=1}^{p-1} |1 - e^{2\pi i s^k q/p}| \ge \left(\frac{p}{k}\right)^k.$$

Proof. Choose integers $\beta_1, \ldots, \beta_k$ such that $\beta_1 + p\mathbb{Z}, \ldots, \beta_k + p\mathbb{Z}$ gives a complete set of representatives of the k cosets of R_k in $(\mathbb{Z}/p\mathbb{Z})^*$. As $(p-1)/k$ is even, it follows that we can choose integers $\alpha_1, \ldots, \alpha_M$ such that $\alpha_1 + p\mathbb{Z}, -\alpha_1 + p\mathbb{Z}, \ldots, \alpha_M + p\mathbb{Z}, -\alpha_M + p\mathbb{Z}$ forms the complete set of elements of R_k. Thus we have

$$(*) \qquad \prod_{s=1}^{p-1} |1 - e^{2\pi i s^k q/p}| = \Big(\prod_{j=1}^{M} (|1 - e^{2\pi i \alpha_j q/p}| \cdot |1 - e^{-2\pi i \alpha_j q/p}|)\Big)^k$$
$$= \Big(\prod_{j=1}^{M} (1 - e^{2\pi i \alpha_j q/p})(1 - e^{-2\pi i \alpha_j q/p})\Big)^k.$$

Now let $R(x) \in \mathbb{Z}[x, x^{-1}]$ be given by $\prod_{j=1}^{M}(1 - x^{\alpha_j})(1 - x^{-\alpha_j})$. It follows easily from $(*)$ that $R(e^{2\pi i q/p}) > 0$ if $1 \le q \le p-1$, and that $R(1) = 0$. Moreover, it is easily shown that for any Laurent polynomial L over $\mathbb{Z}$ and any prime p, one has the fact that $\sum_{j=0}^{p-1} L(e^{2\pi i j/p})$ is an integral multiple of p. Hence from our previous remarks we have $\sum_{j=1}^{p-1} R(e^{2\pi i j/p}) = ps$ for some positive integer s. Notice

$$(**) \qquad \sum_{j=1}^{k} R(e^{2\pi i \beta_j/p}) = \frac{k}{p-1} \sum_{s=1}^{p-1} R(e^{2\pi i s/p}) = \frac{ksp}{p-1}.$$

Also note that $\sum_{j=1}^{k} R(e^{2\pi i \beta_j/p})$ is an algebraic integer. From $(**)$, we see that this sum is also rational. Thus this sum is in fact an integer, and so

$(p-1)/k$ must divide s. It follows that $\sum_{j=1}^{k} R(e^{2\pi i\beta_j/p}) \ge p$. In particular, there exists some l with $1 \le l \le k$ such that $R(e^{2\pi i\beta_l/p}) \ge p/k$. And so from $(*)$ we see that

$$\prod_{j=1}^{p-1} |1 - e^{2\pi i q j^k/p}| \ge \left(\frac{p}{k}\right)^k$$

for some integer q, as required.

LEMMA 2.4. *Let $M \ge 2$ and let $p \equiv 1 \pmod k$ be prime. Then, given $q \in \mathbb{Z}$, $q \not\equiv 0 \pmod p$, we have*

$$\prod_{s=1}^{p-1}\left(1 - \frac{|1-e^{\pi i/(pM)}|}{|1-e^{2\pi i q s^k/p}|}\right) \ge (pe/2)^{(-k\pi\log 2)/M}.$$

Proof. Notice that

$$\frac{|1-e^{\pi i/(pM)}|}{|1-e^{2\pi i q s^k/p}|} \le \frac{|1-e^{\pi i/(2p)}|}{|1-e^{2\pi i/p}|} = \frac{1}{|1+e^{\pi i/(2p)}+e^{\pi i/p}+e^{3\pi i/(2p)}|} \le \frac{1}{2}$$

for $1 \le s \le p-1$. Furthermore, it is easy to see that $1 - x \ge 4^{-x}$ for $0 \le x \le 1/2$. Thus

$$\begin{aligned}
(1)\qquad \prod_{s=1}^{p-1}\left(1 - \frac{|1-e^{\pi i/(pM)}|}{|1-e^{2\pi i q s^k/p}|}\right) &\ge 4^{-|1-e^{\pi i/(pM)}|(\sum_{s=1}^{p-1}|1-e^{2\pi i q s^k/p}|^{-1})}\\
&\ge 4^{-(\pi/(pM))(\sum_{s=1}^{p-1}|2\sin(\pi q s^k/p)|^{-1})}.
\end{aligned}$$

Now let $\beta_1,\ldots,\beta_k$ be integers such that $\beta_1+p\mathbb{Z},\ldots,\beta_k+p\mathbb{Z}$ forms a complete family of representatives of the k cosets of R_k in $(\mathbb{Z}/p\mathbb{Z})^*$. Then there is some i with $1 \le i \le k$ such that

$$\sum_{s=1}^{p-1}\left|2\sin\left(\frac{\pi q s^k}{p}\right)\right|^{-1} = \sum_{s=1}^{p-1}\left|2\sin\left(\frac{\pi \beta_i s^k}{p}\right)\right|^{-1}.$$

Hence

$$\begin{aligned}
&\sum_{s=1}^{p-1}\left|2\sin\left(\frac{\pi q s^k}{p}\right)\right|^{-1}\\
&\quad\le \sum_{j=1}^{k}\sum_{s=1}^{p-1}\left|2\sin\left(\frac{\pi \beta_j s^k}{p}\right)\right|^{-1} = \frac{k}{p-1}\sum_{j=1}^{p-1}\sum_{s=1}^{p-1}\left|2\sin\left(\frac{\pi j s^k}{p}\right)\right|^{-1}\\
&\quad= k\sum_{m=1}^{p-1}\left|2\sin\left(\frac{\pi m}{p}\right)\right|^{-1} \qquad \text{(by changing the order of summation)}
\end{aligned}$$

$$= k \sum_{m=1}^{(p-1)/2} \left(\sin\left(\frac{\pi m}{p}\right)\right)^{-1} \le k \sum_{m=1}^{(p-1)/2} \frac{p}{2m} \quad \text{(by Schwarz's inequality)}$$
$$\le \left(\frac{pk}{2}\right)\left(1+\log\left(\frac{p-1}{2}\right)\right) \le pk\log\left(\frac{ep}{2}\right)\Big/2.$$

By *Schwarz's inequality* we mean the inequality $x/2 \le \sin x \le x$ for $0 \le x \le \pi/2$.

Thus, by (1), we have

$$\prod_{s=1}^{p-1}\left(1-\frac{|1-e^{\pi i/(pM)}|}{|1-e^{2\pi i q s^k/p}|}\right) \ge 4^{-(\pi/(pM))(pk\log(ep/2)/2)} = \left(\frac{ep}{2}\right)^{(-k\pi\log 2)/M}$$

as required.

THEOREM 2.6. *If k is an integer greater than or equal to two then there exists a constant $c > 1$ such that*

$$\max_{x\in S^1}\Big|\prod_{n=1}^{m}(1-x^{n^k})\Big| > c^m$$

for all m sufficiently large.

Proof. Choose a prime p with $p \equiv 1 \pmod{2k}$ and $p > \frac{1}{64}(k^3e^4/8)^k$. By Lemma 2.3, we can choose an integer $q \in \mathbb{Z}$ such that

$$\prod_{j=1}^{p-1}|1-e^{2\pi i q j^k/p}| \ge \left(\frac{p}{k}\right)^k.$$

Let $\varepsilon_N = 1/(7p(pN)^k)$ and $\Theta_N = q/p+\varepsilon_N$ for all $N \in \mathbb{N}$. Notice that

$$(1) \quad \prod_{n=1}^{Np}|1-e^{2\pi i\Theta_N n^k}|$$
$$= \prod_{j=0}^{N-1}\prod_{m=1}^{p-1}|1-e^{2\pi i(pj+m)^k\varepsilon_N}e^{2\pi i q m^k/p}|\prod_{s=1}^{N}|1-e^{2\pi i\varepsilon_N(ps)^k}|.$$

Now

$$\prod_{s=1}^{N}|1-e^{2\pi i\varepsilon_N(ps)^k}|$$
$$= \prod_{s=1}^{N}|2\sin(\pi\varepsilon_N(ps)^k)| \ge \prod_{s=1}^{N}\frac{2}{\pi}2\pi\varepsilon_N(ps)^k \quad \text{(by Schwarz's inequality)}$$
$$= \frac{(4p^k)^N N!^{kN}}{7^N p^N (pN)^{kN}} \ge \frac{4^N}{7^N p^N e^{kN}} \quad \text{(by Stirling's approximation).}$$

Thus, by (1), we have

$$(2)\quad \prod_{n=1}^{Np} |1 - e^{2\pi i \Theta_N n^k}| \geq \left(\frac{4}{7pe^k}\right)^N \prod_{j=0}^{N-1} \prod_{m=1}^{p-1} |1 - e^{2\pi i m^k q/p} e^{2\pi i \varepsilon_N (pj+m)^k}|.$$

Now

$$\begin{aligned}
&|1 - e^{2\pi i m^k q/p} e^{2\pi i \varepsilon_N (pj+m)^k}| \\
&\quad \geq |1 - e^{2\pi i m^k q/p}| - |e^{2\pi i q m^k/p}| \cdot |e^{2\pi i q m^k/p} e^{2\pi i \varepsilon_N (pj+m)^k}| \\
&\quad = |1 - e^{2\pi i m^k q/p}| \left(1 - \frac{|1 - e^{2\pi i \varepsilon_N (pj+m)^k}|}{|1 - e^{2\pi i m^k q/p}|}\right) \\
&\quad \geq |1 - e^{2\pi i m^k q/p}| \left(1 - \frac{|1 - e^{2\pi i/(7p)}|}{|1 - e^{2\pi i m^k q/p}|}\right)
\end{aligned}$$

for $0 \leq j \leq N-1$ and $1 \leq m \leq p-1$ and so

$$\begin{aligned}
&\prod_{j=0}^{N-1} \prod_{m=1}^{p-1} |1 - e^{2\pi i m^k q/p} e^{2\pi i \varepsilon_N (pj+m)^k}| \\
&\quad \geq \prod_{j=0}^{N-1} \prod_{m=1}^{p-1} |1 - e^{2\pi i m^k q/p}| \prod_{j=0}^{N-1} \prod_{m=1}^{p-1} \left(1 - \frac{|1 - e^{2\pi i/(7p)}|}{|1 - e^{2\pi i m^k q/p}|}\right) \\
&\quad \geq \left(\frac{p}{k}\right)^{kN} \left(\frac{ep}{2}\right)^{(-kN\pi \log 2)/7} \qquad \text{(by Lemma 2.4).}
\end{aligned}$$

Thus, by (2), we have

$$\begin{aligned}
\prod_{n=1}^{Np} |1 - e^{2\pi i \Theta_N n^k}| &\geq \left(\frac{4}{pe^k}\right)^N \left(\frac{p^{1-(\pi \log 2)/7}}{k}\right)^{kN} \left(\frac{2}{e}\right)^{(kN\pi \log 2)/7} \\
&\geq \frac{4^N}{p^N e^{kN}} \cdot \frac{p^{2kN/3}}{k^{kN}} \left(\frac{2}{e}\right)^{kN/3} \geq \left[\left(\frac{4p^{1/3}}{e^k k^k} \left(\frac{2}{e}\right)^{k/3}\right)^{1/p}\right]^{pN}.
\end{aligned}$$

Now let

$$C = \left(\frac{4p^{1/3}}{e^k k^k} \left(\frac{2}{e}\right)^{k/3}\right)^{1/p}.$$

Note that $C > 1$ as $p > \frac{1}{64}(k^3 e^4/8)^k$. Now let $\varepsilon > 0$. Choose c satisfying $C > c > 1$. Then notice that given $m \in \mathbb{N}$, we can find a positive integer N such that $(N-1)p < m \leq Np$. Then

$$\begin{aligned}
\prod_{j=1}^{m} |1 - e^{2\pi i \Theta_N j^k}| &= \Big(\prod_{j=1}^{Np} |1 - e^{2\pi i \Theta_N j^k}|\Big) \Big/ \Big(\prod_{j=m+1}^{Np} |1 - e^{2\pi i \Theta_N j^k}|\Big) \\
&\geq C^{Np}/2^{Np-m} \geq 2^{-p} C^m \geq c^m \quad \text{(for sufficiently large } m\text{).}
\end{aligned}$$

We now consider sequences $\{m_j\}$ in which $m_j = aj^2 + bj + c$ for all $j \in \mathbb{N}$, where a, b, and c are elements of $\mathbb{Q}$ such that $m_j \in \mathbb{N}$ for all $j \in \mathbb{N}$. We show that for such sequences, the maximum obtained by $\prod_{j=0}^{n}|1-z^{m_j}|$ on the unit circle of the complex plane grows at an exponential rate with respect to n, as n tends to infinity. Note that it is no loss of generality to assume that $\{m_j\}$ forms an increasing sequence of natural numbers, as our sequence must be eventually increasing.

LEMMA 2.5. *Let* $p \equiv 61 \pmod{120}$ *and let* k *be a quadratic non-residue modulo* p *and let* $\varepsilon > 0$. *Then*

$$\prod_{\substack{s=0\\ ks^2\not\equiv -2\,(\mathrm{mod}\,p)}}^{p-1} |1-e^{2\pi i(ks^2+2)/p}| > e^{p^{1/2-\varepsilon}}$$

for all sufficiently large primes p.

Proof. As $p \equiv 61 \pmod{120}$, it follows that $\pm1, \pm3, \pm4, \pm5$ are quadratic residues mod p. Thus if $ks^2 \not\equiv \pm 2 \pmod{p}$, then

$$|1-e^{2\pi i ks^2/p}| > |1-e^{12\pi i/p}|,$$

and so

$$\frac{|1-e^{2\pi i(ks^2+2)/p}|}{|1-e^{2\pi iks^2/p}|} \ge \left(1-\frac{|1-e^{4\pi i/p}|}{|1-e^{12\pi i/p}|}\right) \ge \frac{1}{2}.$$

Recall that $1-x \ge 4^{-x}$ for $0 \le x \le 1/2$, and so we have

$$(*)\qquad \prod_{\substack{s=1\\ ks^2\not\equiv \pm 2\,(\mathrm{mod} p)}}^{p-1} \left(1-\frac{|1-e^{4\pi i/p}|}{|1-e^{2\pi iks^2/p}|}\right) \ge 4^{-(4\pi/p)\sum_{s=1}^{p-1}|2\sin(\pi ks^2/p)|^{-1}}.$$

Notice that given an integer j, as s runs through the values $1,\ldots,p$, the congruence $ks^2 \equiv j \pmod{p}$ has at most 2 solutions. We may use this fact and equation $(*)$, to obtain

$$(**)\qquad \prod_{\substack{s=1\\ ks^2\not\equiv \pm 2\,(\mathrm{mod}\,p)}}^{p-1} \left(1-\frac{|1-e^{4\pi i/p}|}{|1-e^{2\pi iks^2/p}|}\right)$$
$$\ge 4^{-(4\pi/p)\sum_{j=1}^{(p-1)/2}(|\sin(\pi j/p)|^{-1}+|\sin(-\pi j/p)|^{-1})}$$
$$\ge 4^{-(4\pi/p)\sum_{j=1}^{(p-1)/2}(p/(2j))} \qquad \text{(by Schwarz's inequality)}$$
$$\ge 4^{-4\pi(\log(p/2)+1)}$$
$$= \left(\frac{pe}{2}\right)^{-4\pi\log 4}.$$

Notice that the congruences $ks^2 \equiv 0 \pmod p$ and $ks^2 \equiv 2 \pmod p$ have respectively 1 solution and 2 solutions mod p. Thus

$$(\dagger)\qquad \prod_{\substack{s=0\\ ks^2\not\equiv -2\,(\mathrm{mod}\,p)}}^{p-1} |1-e^{2\pi i(ks^2+2)/p}|$$

$$\ge \left|2\sin\left(\frac{2\pi}{p}\right)\right|\cdot\left|2\sin\left(\frac{4\pi}{p}\right)\right|^2$$

$$\times \prod_{\substack{s=1\\ ks^2\not\equiv \pm 2\,(\mathrm{mod}\,p)}}^{p-1} |1-e^{2\pi iks^2/p}|\left(1-\frac{|1-e^{4\pi i/p}|}{|1-e^{2\pi iks^2/p}|}\right)$$

$$\ge \frac{|2\sin(2\pi/p)|\cdot|2\sin(4\pi/p)|^2}{|2\sin(2\pi/p)|^2|2\sin(-2\pi/p)|^2}\left(\frac{pe}{2}\right)^{-4\pi\log 4}\prod_{s=1}^{p-1}|1-e^{2\pi iks^2/p}| \qquad (\text{by } (**))$$

$$\ge \left(\frac{pe}{2}\right)^{-4\pi\log 4}\frac{(8/p)(16/p)^2}{(4\pi/p)^2(4\pi/p)^2}\Bigg(\prod_{\substack{n=1\\ (\frac{n}{p})=-1}}^{p-1} 2\sin\left(\frac{\pi n}{p}\right)\Bigg)^2,$$

where the last step again follows by the Schwarz inequality.

Let $L(s,\chi_p)$ denote the sum $\sum_{j=1}^{\infty}\left(\frac{j}{p}\right)/j^s$ for $\Re s\ge 1$. It is known from the work of Dirichlet (see Davenport [5]) that for $p\equiv 1 \pmod 4$,

$$(\mathrm{i})\qquad \Bigg(\prod_{\substack{n=1\\ (\frac{n}{p})=-1}}^{p-1} 2\sin\left(\frac{\pi n}{p}\right)\Bigg)\Bigg/\Bigg(\prod_{\substack{r=1\\ (\frac{r}{p})=1}}^{p-1} 2\sin\left(\frac{\pi r}{p}\right)\Bigg) = \exp(\sqrt{p}L(1,\chi_p)).$$

We also note the classical identity:

$$(\mathrm{ii})\qquad \prod_{\substack{n=1\\ (\frac{n}{p})=-1}}^{p-1} 2\sin\left(\frac{\pi n}{p}\right)\prod_{\substack{r=1\\ (\frac{n}{p})=1}}^{p-1} 2\sin\left(\frac{\pi r}{p}\right) = \prod_{j=1}^{p-1} 2\sin\left(\frac{\pi j}{p}\right) = p.$$

Combining (i) and (ii) yields

$$\prod_{\substack{n=1\\ (\frac{n}{p})=-1}}^{p-1} 2\sin\left(\frac{\pi n}{p}\right) = \sqrt{p}e^{\sqrt{p}L(1,\chi_p)/2} \qquad \text{for } p\equiv 1 \pmod 4.$$

Moreover, Siegel [15] was able to show that given $\varepsilon>0$, we have $L(1,\chi_p)> p^{-\varepsilon}$ for all primes p sufficiently large. Combining these two facts with (†) gives the result.

THEOREM 2.7. *Let $f(x)=ax^2+bx+c$ be a quadratic polynomial such that $\{f(n)\}_{n\in\mathbb{N}}$ forms a non-decreasing sequence of positive integers. Then* *there exists some* $c>1$ *such that*

$$\max_{x\in S^1}\prod_{j=1}^{n}|1-x^{f(j)}| > c^n$$

for all n *sufficiently large.*

Proof. As the restriction of f to $\mathbb{Z}$ gives a map from the integers into itself, it follows that $2a, 2b$, and c must all be integers. In light of the previous theorem, we may assume that $b^2-4ac\neq 0$. Notice also that $\lim_{x\to\infty} f(x)/x^2 = a > 0$, and as $f(n)>0$ for all $n\in\mathbb{N}$, it follows that there exists some positive constants C_1, C_2 such that $C_2n^2 > f(n) > C_1n^2$ for all $n\in\mathbb{N}$.

By Lemma 2.5 we may choose a prime $p\equiv 61 \pmod{120}$ such that

$$\prod_{\substack{k=1\\ \alpha k^2\not\equiv -2 \,(\mathrm{mod}\, p)}}^{p} |1-e^{2\pi i(\alpha k^2+2)/p}| > e^{\sqrt[3]{p}}$$

whenever α is a quadratic non-residue mod p. We also insist that

$$\frac{C_1^2 e^{\sqrt[3]{p}}}{16C_2^2p^3e^4}\left(\frac{pe}{2}\right)^{-\pi\log 2} > 1$$

and

$$p\not\equiv a, b^2-4ac \pmod{p}.$$

Let a^* be the multiplicative inverse of a mod p. Then

$$an^2+bn+c\equiv a\left(n+ba^*\left(\frac{p+1}{2}\right)\right)^2+\left(\frac{p-1}{4}\right)b^2a^*+c \pmod{p}.$$

It follows that there is some integer d, with $p\nmid d$, such that the sets

$$\{d, a+d, 4a+d, 9a+d, \ldots, (p-1)^2a+d\}$$

and

$$\{f(0), f(1), f(2), \ldots, f(p-1)\}$$

are just permutations of one another when considered mod p. Now, notice that if $\left(\frac{da^*}{p}\right)=-1$, then $f(x)$ has no roots mod p, and so by appealing to Lemma 2.2 we can see that the result will hold. Thus we may assume that $\left(\frac{da^*}{p}\right)=+1$. Now choose q such that $qd\equiv 2 \pmod{p}$. Note

$$\left(\frac{qa}{p}\right)=\left(\frac{qa}{p}\right)\left(\frac{a^*d}{p}\right)=\left(\frac{qd}{p}\right)=\left(\frac{2}{p}\right)=-1.$$

Let $\varepsilon_N = 1/(4C_2p^3N^2)$ and $\Theta_N = q/p+\varepsilon_N$. Then

$$\begin{aligned}
(1)\quad &\prod_{s=1}^{Np} |1 - e^{2\pi i \Theta_N f(s)}| \\
&\geq \prod_{\substack{j=1 \\ f(j)\equiv 0 \,(\mathrm{mod}\, p)}}^{Np} |1 - e^{2\pi i \varepsilon_N f(j)}| \\
&\quad \times \prod_{\substack{k=1 \\ f(k)\not\equiv 0 \,(\mathrm{mod}\, p)}}^{Np} |1 - e^{2\pi i q f(k)/p}| \left(1 - \frac{|1 - e^{2\pi i f(k)\varepsilon_N}|}{|1 - e^{2\pi i q f(k)/p}|}\right) \\
&\geq \prod_{\substack{j=1 \\ f(j)\equiv 0 \,(\mathrm{mod}\, p)}}^{Np} |2\sin(\pi f(j)\varepsilon_N)| \\
&\quad \times \left(\prod_{\substack{k=1 \\ ak^2\not\equiv -d \,(\mathrm{mod}\, p)}}^{p} |1 - e^{2\pi i q(ak^2+d)/p}| \left(1 - \frac{|1 - e^{2\pi i C_2 (Np)^2 \varepsilon_N}|}{|1 - e^{2\pi i q(ak^2+d)/p}|}\right)\right)^N \\
&\geq \prod_{\substack{j=1 \\ f(j)\equiv 0 \,(\mathrm{mod}\, p)}}^{Np} (4 f(j)\varepsilon_N) \\
&\quad \times \left(\prod_{\substack{k=1 \\ qak^2\not\equiv -2 \,(\mathrm{mod}\, p)}}^{p} |1 - e^{2\pi i (qak^2+2)/p}| \left(1 - \frac{|1 - e^{2\pi i C_2 (Np)^2 \varepsilon_N}|}{|1 - e^{2\pi i (qak^2+2)/p}|}\right)\right)^N \\
&\geq \prod_{\substack{j=1 \\ f(j)\equiv 0 \,(\mathrm{mod}\, p)}}^{Np} (4 f(j)\varepsilon_N) \left(e^{\sqrt[3]{p}} \prod_{\substack{k=1 \\ qak^2\not\equiv -2 \,(\mathrm{mod}\, p)}}^{p} \left(1 - \frac{|1 - e^{2\pi i C_2 (Np)^2 \varepsilon_N}|}{|1 - e^{2\pi i (qak^2+2)/p}|}\right)\right)^N,
\end{aligned}$$

where the penultimate step follows from Schwarz's inequality. Now notice that

$$\frac{|1 - e^{2\pi i C_2 (Np)^2 \varepsilon_N}|}{|1 - e^{2\pi i (qak^2+2)/p}|} \leq \frac{|1 - e^{\pi i/(2p)}|}{|1 - e^{2\pi i/p}|} \leq \frac{1}{2}.$$

And so we may again appeal to the fact that $1-x \geq 4^{-x}$ for $0 \leq x \leq 1/2$ and the fact that for any given integer r, the congruence $qak^2 + 2 \equiv r \pmod{p}$ has at most two solutions mod p, and use the same type of argument that was employed in deriving $(**)$ in Lemma 2.5, to obtain

$$(2)\qquad \prod_{\substack{k=1 \\ qak^2\not\equiv -2 \,(\mathrm{mod}\, p)}}^{p} \left(1 - \frac{|1 - e^{2\pi i C_2 (Np)^2 \varepsilon_N}|}{|1 - e^{2\pi i (qak^2+2)/p}|}\right) \geq \left(\frac{pe}{2}\right)^{-\pi \log 2}.$$

Substituting the information from (2) into (1), we obtain

$$(3)\quad \prod_{s=1}^{Np}|1-e^{2\pi i\Theta_N f(s)}| \ge \prod_{\substack{j=1\\ f(j)\equiv 0\ (\mathrm{mod}\ p)}}^{Np}(4f(j)\varepsilon_N)\left(e^{\sqrt[3]{p}}\left(\frac{pe}{2}\right)^{-\pi\log 2}\right)^N.$$

Finally, notice that $f(x)$ has at mod 2 roots mod p, and so

$$(4)\quad \prod_{\substack{j=0\\ f(j)\equiv 0\ (\mathrm{mod}\ p)}}^{Np}(4f(j)\varepsilon_N)$$
$$\ge (4\varepsilon_N)^{2N}\prod_{n=0}^{N-1}(C_1(1+pn)^2)^2$$
$$\ge (4C_1\varepsilon_N)^{2N}(p^{-2}N^{-4})\prod_{m=1}^{N}(pm)^4$$
$$\ge (4C_1\varepsilon_N)^{2N}(p^{-2}N^{-4})\left(\frac{p^{4N}N^{4N}}{e^{4N}}\right)\qquad\text{(Stirling's formula)}$$
$$=\left(\frac{C_1^2}{C_2^2p^2e^4}\right)^N p^{-2}N^{-4}\ge\left(\frac{C_1^2}{16C_2^2p^3e^4}\right)^N,$$

where the last step follows from the inequalities $p^{-2}\ge p^{-2N}$ and $2^N\ge N$.

We define

$$C=\left(\frac{C_1^2e^{\sqrt[3]{p}}}{16C_2^2p^3e^4}\left(\frac{pe}{2}\right)^{-\pi\log 2}\right)^{1/p}.$$

Notice p has been chosen so that $C>1$. Choose some c satisfying $C>c>1$. We now combine (3) with (4) to obtain

$$\prod_{s=1}^{Np}|1-e^{2\pi i\Theta_N f(s)}|\ \ge\left(\left(\frac{C_1^2e^{\sqrt[3]{p}}}{16C_2^2p^3e^4}\left(\frac{pe}{2}\right)^{-\pi\log 2}\right)^{1/p}\right)^{pN}=C^{pN}.$$

Let m be a given positive integer. Just as in Theorem 2.7, it is easily shown that

$$\max_{z\in S^1}\prod_{s=1}^{m}|1-z^{f(s)}|\ge 2^{-p}C^m\ge c^m$$

for all m sufficiently large, as required.

Acknowledgements. Lemma 2.2 is primarily due to L. Szekely and we would like to thank S. V. Konyagin and A. M. Odlyzko for their comments.

References

[1] F. V. Atkinson, *On a problem of Erdős and Szekeres*, Canad. Math. Bull. 4 (1961), 7–12.

[2] A. S. Belov and S. V. Konyagin, *On estimates for the constant term of a nonnegative trigonometric polynomial with integral coefficients*, Mat. Zametki 59 (1996), 627–629 (in Russian).

[3] P. Borwein, *Some restricted partition functions*, J. Number Theory 45 (1993), 228–240.

[4] P. Borwein and C. Ingalls, *The Prouhet*, *Tarry*, *Escott problem*, Enseign. Math. 40 (1994), 3–27.

[5] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer, 1980.

[6] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.

[7] P. Erdős, *Problems and results on diophantine approximation*, in: Asymptotic Distribution Modulo 1, J. F. Koksma and L. Kuipers (eds.), Noordhoff, 1962.

[8] P. Erdős and G. Szekeres, *On the product* $\prod_{k=1}^{n}(1-z^{a_k})$, Publ. Inst. Math. (Beograd) 13 (1959), 29–34.

[9] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford, 1979.

[10] M. N. Kolountzakis, *On nonnegative cosine polynomials with nonnegative integral coefficients*, Proc. Amer. Math. Soc. 120 (1994), 157–163.

[11] R. Maltby, *Root systems and the Erdős–Szekeres Problem*, Acta Arith. 81 (1997), 229–245.

[12] A. M. Odlyzko, *Minima of cosine sums and maxima of polynomials on the unit circle*, J. London Math. Soc. (2) 26 (1982), 412–420.

[13] A. M. Odlyzko and L. B. Richmond, *On the unimodality of some partition polynomials*, European J. Combin. 3 (1982), 69–84.

[14] K. F. Roth and G. Szekeres, *Some asymptotic formulae in the theory of partitions*, Quart. J. Math. Oxford Ser. (2) 5 (1954), 241–259.

[15] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), 83–86.

[16] C. Sudler, *An estimate for a restricted partition function*, Quart. J. Math. Oxford Ser. (2) 15 (1964), 1–10.

[17] E. M. Wright, *Proof of a conjecture of Sudler*, ibid., 11–15.

[18] —, *A closer estimation for a restricted partition function*, ibid., 283–287.

Pure Mathematics Student
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1
E-mail: bell@scylla.math.mcgill.ca

Department of Mathematics and Statistics
Simon Fraser University
Burnaby, British Columbia
Canada V5A 1S6
E-mail: pborwein@math.sfu.ca

Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1
E-mail: lbrichmond@dragon.uwaterloo.ca

Received on 19.8.1997
and in revised form on 20.2.1998 (3245)