Publ. Math. Debrecen
Manuscript (October 26, 2010)

Primitive sets with large counting functions

By Greg Martin and Carl Pomerance

Dedicated to András Sárközy on his 70th birthday

Abstract. A set of positive integers is said to be primitive if no element of the set is a multiple of another. If $\mathcal{S}$ is a primitive set and $S(x)$ is the number of elements of $\mathcal{S}$ not exceeding x, then a result of Erdős implies that $\int_2^\infty (S(t)/t^2 \log t)\, dt$ converges. We establish an approximate converse to this theorem, showing that if F satisfies some mild conditions and $\int_2^\infty (F(t)/t^2 \log t)\, dt$ converges, then there is a primitive set $\mathcal{S}$ with $S(x) \asymp F(x)$.

1. Introduction

A set of positive integers is *primitive* if no element of the set is a multiple of another. In the 1930s Chowla, Davenport, and Erdős independently studied a special primitive set, namely the set of primitive nondeficient numbers (numbers n such that the sum of the proper divisors of n is at least n, but no proper divisor of n has this property), which probably inspired the generalization to general primitive sets around the same time. Besicovitch [2] showed, perhaps unexpectedly, that the upper asymptotic density of a primitive set can be arbitrarily close to $1/2$; his construction yields a set whose counting function is occasionally large but usually extremely small. In [3], Erdős showed that the lower asymptotic density

Mathematics Subject Classification: 11B05.
Key words and phrases: primitive sets, sequences and sets.
The first author was supported in part by grants from the Natural Sciences and Engineering Research Council of Canada. The second author was supported in part by NSF grant DMS-0703850.

of a primitive set must be 0, and also that

$$\sup_{\mathcal{S} \text{ primitive}} \sum_{n \in \mathcal{S} \setminus \{1\}} \frac{1}{n \log n} < \infty. \tag{1}$$

It is thought that this supremum is attained when $\mathcal{S}$ is the set of primes, but this is still not known. Further references to results on primitive sets can be found in [6], [10, Section 5.1], and [11, Section 5].

In this note we ask if there are primitive sets with consistently large counting functions (as opposed to occasionally large counting functions, as in Besicovitch's example). We show that essentially any smoothly growing counting function that is consistent with the necessary convergence (1) can be the order of magnitude for the counting function of a primitive set.

A favorite problem of Erdős, as related in [5], is as follows: If $1 < b_1 < b_2 < \dots$ is a sequence of numbers with $\sum 1/b_n \log b_n < \infty$, must there exist a primitive sequence $1 < a_1 < a_2 < \dots$ with $a_n \ll b_n$? One may interpret our principal result as answering "yes" for smoothly growing sequences $\{b_n\}$.

For a set $\mathcal{S}$ of natural numbers, let $S(x)$ denote its counting function; that is, $S(x)$ is the number of members of $\mathcal{S}$ not exceeding x. Let $\log_1 x = \max\{1, \log x\}$ and $\log_\ell x = \log_1(\log_{\ell-1} x)$ for every integer $\ell \ge 2$.

Theorem 1. *Suppose that $L(x)$ is defined, positive, and increasing for $x \ge 2$, that $L(2x) \sim L(x)$ as $x \to \infty$, and that*

$$\int_2^\infty \frac{dt}{t \log t \cdot L(t)} < \infty. \tag{2}$$

Then there is a primitive set $\mathcal{S}$ such that

$$S(x) \asymp \frac{x}{\log_2 x \cdot \log_3 x \cdot L(\log_2 x)} \tag{3}$$

for all sufficiently large x. In particular, for any integer $\ell \ge 3$ and every real number $\varepsilon > 0$, there exists a primitive set $\mathcal{S}$ such that

$$S(x) \asymp \frac{x}{\log_2 x \cdots \log_{\ell-1} x \cdot (\log_\ell x)^{1+\varepsilon}} \tag{4}$$

for all sufficiently large x.

By taking $L(x) = (\log_2 x) \cdots (\log_{\ell-3} x)(\log_{\ell-2} x)^{1+\varepsilon}$, we see that (3) implies (4) for $\ell \ge 4$, and the case $\ell = 3$ follows by taking $L(x) = (\log x)^\varepsilon$. By an argument somewhat similar to our proof of Theorem 1, Ahlswede, Khachatrian,

and Sárközy [1] gave a construction for the lower bound in (4) in the case $\ell = 3$. Like the paper [1], our proof depends heavily on a result of Sathe–Selberg on the fine distribution of integers with a given number of prime factors.

It is not hard to see that the condition (2) is necessary in Theorem 1. Indeed, suppose $\mathcal{S}$ is a set of natural numbers greater than 1 satisfying (3), and suppose that $\sum_{n\in\mathcal{S}\setminus\{1\}} 1/(n\log n)$ converges (as it must, by equation (1), for primitive sets $\mathcal{S}$). Since

$$\sum_{n\in\mathcal{S}\setminus\{1\}} \frac{1}{n\log n} = \int_2^\infty S(t)\left(\frac{1}{t^2\log t} + \frac{1}{t^2\log^2 t}\right)\,dt,$$

it follows that

$$\int_2^\infty \frac{S(t)}{t^2\log t}\,dt < \infty.$$

Then (3) implies that

$$\int_2^\infty \frac{dt}{t\log t\cdot\log_2 t\cdot\log_3 t\cdot L(\log_2 t)}\,dt < \infty.$$

Via a change of variables, we obtain (2).

Another question one might consider is what conditions on the distribution of a set $\mathcal{A}$ of natural numbers forces $\mathcal{A}$ to have a large primitive subset. It is not too difficult to see that if an infinite set $\mathcal{A}$ contains no primitive subset of size k, then $A(x) \ll k\log x$. Indeed, if $b_1 < \cdots < b_k$ are any k consecutive elements in $\mathcal{A}$, that they are not primitive forces some $b_i \mid b_j$ for $1 \le i < j \le k$, so that $b_k/b_1 \ge 2$. On the other hand, the set $\mathcal{A} = \{m2^j : m < 2k-1, j \ge 0\}$ has no primitive subset of size k and $A(x) \gg k\log x$.

At the other extreme, it is also not difficult to see that if $\mathcal{A}$ has positive upper density, then it contains a primitive subset also with positive upper density. Indeed, any integer subset of a dyadic interval $[x, 2x)$ is primitive, and a set with positive upper density must contain a fixed positive proportion δ of each dyadic interval $[x_i, 2x_i)$ for some unbounded sequence $\{x_i\}$. The Besicovitch argument then goes over to show that $\mathcal{A}$ contains a primitive subset of upper density arbitrarily close to $\delta/2$.

We address this subset question for a set of "intermediate" density, namely it has density 0, but an infinite reciprocal sum. We prove the following result.

Theorem 2. *There is a set $\mathcal{A}$ of natural numbers of asymptotic density 0 satisfying*

$$\sum_{a\in\mathcal{A}\setminus\{1\}} \frac{1}{a\log a} < \infty \quad \textit{and} \quad \sum_{a\in\mathcal{A}} \frac{1}{a} = \infty, \tag{5}$$

such that for any primitive set $\mathcal{S}$ contained in $\mathcal{A}$ we have

$$\sum_{s\in\mathcal{S}} \frac{1}{s} < \infty. \tag{6}$$

In particular, no primitive subset of $\mathcal{A}$ has positive relative lower density in $\mathcal{A}$, despite the counting function of $\mathcal{A}$ being small enough to allow the possibility. The set $\mathcal{A}$ that we exhibit has the property that there is a primitive subset of relative positive upper density, so there remains a perhaps interesting problem: Is there a set $\mathcal{A}$ with infinite reciprocal sum such that any primitive subset has relative density 0 in $\mathcal{A}$? Maybe the Besicovitch construction will show such a set $\mathcal{A}$ does not exist.

2. Constructing primitive sets from a sequence of primes

Let $p_1 < p_2 < \cdots$ be any infinite sequence of primes such that

$$\sum_{j=1}^{\infty} \frac{1}{p_j} < \frac{1}{2}.$$

We need this sequence not to grow too quickly; for now we make only the restriction $p_j \ll j^2$.

Using the usual notation $\Omega(n)$ for the number of prime factors of n counted with multiplicity, we define for any positive integer k

$$\mathcal{S}_k = \{n \in \mathbb{N}\colon \Omega(n) = k,\, p_k \mid n,\, (p_1\cdots p_{k-1}, n) = 1\},$$

and we set

$$\mathcal{S} = \bigcup_{k=1}^{\infty} \mathcal{S}_k.$$

We prove two results about $\mathcal{S}$: the first is that $\mathcal{S}$ is primitive and the second is a lower bound for $S(x)$ (see Proposition 6 below).

Lemma 3. *The set $\mathcal{S}$ is primitive.*

Proof. Note that if m and n are distinct positive integers and m divides n, then $\Omega(m) < \Omega(n)$. Therefore if $\mathcal{S}$ were not primitive, then there would exist positive integers $j < k$ and integers $m \in \mathcal{S}_j$ and $n \in \mathcal{S}_k$ such that $m \mid n$. However, then p_j would divide m but not n, a contradiction. (Indeed, $\mathcal{S}$ is an example of a homogeneous set, in the terminology of [12].) □

Let $\sigma_j(x)$ denote the number of positive integers $n \le x$ such that $\Omega(n) = j$.

Lemma 4 (Sathe–Selberg)**.** *For any positive integer $j \le \lfloor \frac{3}{2} \log_2 x \rfloor$,*

$$\sigma_j(x) = H_j(x) \left(1 + O\left(\frac{1}{\log_2 x}\right)\right)$$

where

$$H_j(x) = G\bigg(\frac{j-1}{\log\log x}\bigg) \frac{x}{\log x} \frac{(\log\log x)^{j-1}}{(j-1)!}$$

and

$$G(z) = \frac{1}{\Gamma(z+1)} \prod_p \left(1 - \frac{z}{p}\right)^{-1} \left(1 - \frac{1}{p}\right)^z.$$

For a proof, see [8, Theorem 7.19].

Lemma 5. *Let x be a sufficiently large real number. For any integer $k \in [2, \frac{3}{2} \log_2 x]$,*

$$S_k(x) \asymp \frac{x}{\log x} \frac{(\log\log x)^{k-2}}{(k-2)!} \frac{1}{p_k},$$

where the implied constants are absolute.

Proof. The result follows immediately from the prime number theorem in the case $k = 2$, so assume that $k \ge 3$. Since every element of $S_k(x)$ is divisible by p_k and is coprime to $p_1 \dots p_{k-1}$, we have the inequalities

$$\sigma_{k-1}\left(\frac{x}{p_k}\right) \ge S_k(x) \ge \sigma_{k-1}\left(\frac{x}{p_k}\right) - \sum_{j=1}^{k-1} \sigma_{k-2}\left(\frac{x}{p_j p_k}\right).$$

By Lemma 4, this becomes

$$\begin{aligned} H_{k-1}\left(\frac{x}{p_k}\right)\left(1 + O\left(\frac{1}{\log_2(x/p_k)}\right)\right) &\ge S_k(x) \\ &\ge \left(H_{k-1}\left(\frac{x}{p_k}\right) - \sum_{j=1}^{k-1} H_{k-2}\left(\frac{x}{p_j p_k}\right)\right)\left(1 + O\left(\frac{1}{\log_2(x/p_j p_k)}\right)\right). \end{aligned}$$

Because $k \ll \log_2 x$ and $p_j \ll j^2$, each occurrence of $\log(x/p_k)$ or $\log(x/p_j p_k)$ can be rewritten as $(\log x)(1+O(1/\log_2 x))$, and similarly $\log_2(x/p_k)$ and $\log_2(x/p_j p_k)$

can be rewritten as $(\log_2 x)(1+O(1/\log x))$. In addition, the expressions $G((k-2)/\log_2(x/p_k))$ and $G((k-3)/\log_2(x/p_jp_k))$ can be rewritten as

$$G\left(\frac{k-2}{\log_2 x}+O\left(\frac{1}{\log_2 x}\right)\right)=G\left(\frac{k-2}{\log_2 x}\right)\left(1+O\left(\frac{1}{\log_2 x}\right)\right),$$

since $\log G(z)$ is analytic and hence has a bounded first derivative in a neighborhood of the interval $[0,3/2]$. Therefore

$$\begin{aligned}H_{k-1}\left(\frac{x}{p_k}\right)\left(1+O\left(\frac{1}{\log_2 x}\right)\right) &\ge S_k(x)\\ &\ge H_{k-1}\left(\frac{x}{p_k}\right)\left(1-\frac{k-3}{\log_2 x}\sum_{j=1}^{k-1}\frac{1}{p_j}\right)\left(1+O\left(\frac{1}{\log_2 x}\right)\right).\end{aligned}$$

Since the sum is less than $\frac12$, and since $G(z)$ is bounded away from 0 and ∞ on the interval $[0,3/2]$, this becomes

$$S_k(x)\asymp H_{k-1}\left(\frac{x}{p_k}\right)\asymp\frac{x}{\log x}\frac{(\log\log x)^{k-2}}{(k-2)!}\frac{1}{p_k}$$

as claimed. □

Proposition 6. *For $x\ge p_1$, we have $x/p_B\gg S(x)\gg x/p_{B'}$, where $B=B(x)=\lfloor\frac12\log_2 x\rfloor$ and $B'=B'(x)=\lfloor\frac32\log_2 x\rfloor$.*

Proof. Since $\mathcal{S}=\bigcup_{k=1}^\infty\mathcal{S}_k$ is a disjoint union, we have by Lemma 5,

$$S(x)\ge\sum_{k=2}^{B'}S_k(x)\gg\sum_{k=2}^{B'}\frac{x}{\log x}\frac{(\log_2 x)^{k-2}}{(k-2)!}\frac{1}{p_k}\ge\frac{x}{\log x}\frac{1}{p_{B'}}\sum_{k=2}^{B'}\frac{(\log_2 x)^{k-2}}{(k-2)!}\gg\frac{x}{p_{B'}},$$

where we used the inequality

$$\sum_{j=0}^{\lfloor y\rfloor}\frac{y^j}{j!}\gg e^y$$

(which follows from [9, equation 1.10] with $\beta=0$) for the last step. For the upper bound, we have

$$S(x)\le\sum_{k=1}^{\infty}S_k(x)\le\sum_{k=B+1}^{B'}S_k(x)+\sum_{\substack{n\le x\\ \Omega(n)\le B}}1+\sum_{\substack{n\le x\\ \Omega(n)>B'}}1.$$

There is a positive constant c such that the last two sums here are $O(x/(\log x)^c)$. Indeed, $\Omega(n) \le B$ implies that $\omega(n) \le B$, where ω counts the number of distinct prime divisors, so the estimate for $\Omega(n) \le B$ follows from the Hardy–Ramanujan inequality (see [4, Proposition 3]). If $\Omega(n) > B'$, a similar estimate holds using the Hardy–Ramanujan inequality plus an estimate for those n with $\Omega(n) - \omega(n)$ large, or more directly from [7, Lemma 13].

By Lemma 5,

$$\sum_{k=B+1}^{B'} S_k(x) \ll \sum_{k=B+1}^{B'} \frac{x}{\log x} \frac{(\log_2 x)^{k-2}}{(k-2)!} \frac{1}{p_B} \le \frac{x}{p_B} \sum_{j=0}^{\infty} \frac{(\log_2 x)^j}{j! \log x} = \frac{x}{p_B}.$$

Since $p_B \le p_{B'} = O(B'^2) = O((\log_2 x)^2)$, sets of size $O(x/(\log x)^c)$ are negligible, and our result follows. □

3. Proof of Theorem 1

Lemma 7. *Suppose that $L(x)$ is defined, positive, and increasing for $x \ge 2$ and that $L(2x) \sim L(x)$ as $x \to \infty$. Then $L(x) \ll_\varepsilon x^\varepsilon$ for any $\varepsilon > 0$.*

Proof. Given $\varepsilon > 0$, we need to show that $L(x)/x^\varepsilon$ is bounded. Since $L(2x) \sim L(x)$, we may choose x_1 such that $L(2x) < (1 + \varepsilon \log 2) L(x)$ for all $x \ge x_1$. Define $M_u = \max_{u \le x \le 2u} L(x)/x^\varepsilon$. Then for any $u \ge x_1$,

$$M_{2u} = \max_{2u \le x \le 4u} \frac{L(x)}{x^\varepsilon} = \max_{u \le y \le 2u} \frac{L(2y)}{(2y)^\varepsilon} < \frac{1 + \varepsilon \log 2}{2^\varepsilon} \max_{u \le y \le 2u} \frac{L(y)}{y^\varepsilon} < 1 \cdot M_u,$$

since $2^\varepsilon > 1 + \varepsilon \log 2$. Therefore $M_{x_1} > M_{2x_1} > M_{4x_1} > \cdots$, and so $L(x)/x^\varepsilon$ is bounded by M_{x_1} on $[x_1, \infty)$. Since it is clearly bounded by $L(x_1)$ on $[2, x_1]$, the lemma is established. □

Proposition 8. *Suppose that $L(x)$ is defined, positive, and increasing for $x \ge 2$, that $L(2x) \sim L(x)$ as $x \to \infty$, and that*

$$\int_2^\infty \frac{dt}{t \log t \cdot L(t)} < \infty.$$

Then there is a sequence $p_1 < p_2 < \cdots$ of primes with $\sum_{k=1}^\infty 1/p_k < 1/2$ and $p_k \sim k \log k \cdot L(k)$ as $k \to \infty$.

PROOF. Choosing y_0 so that $L(y) \ge 1$ holds for all $y \ge y_0$, define

$$q_k = \begin{cases} \text{the } k\text{th prime}, & \text{if } k < y_0, \\ \text{the } \lfloor kL(k) \rfloor \text{th prime}, & \text{if } k \ge y_0. \end{cases}$$

Then $\{q_k\}$ is increasing since $(k+1)L(k+1) \ge (k+1)L(k) \ge kL(k)+1$ for $k \ge y_0$, so that $\lfloor (k+1)L(k+1) \rfloor > \lfloor kL(k) \rfloor$. By the prime number theorem, when $k \to \infty$ we have

$$q_k \sim \lfloor kL(k) \rfloor \log \lfloor kL(k) \rfloor \sim kL(k)(\log k + \log L(k)) \sim kL(k) \log k,$$

where the last asymptotic equality used Lemma 7. Further,

$$\sum_{k \ge y_0+1} \frac{1}{q_k} \ll \sum_{k \ge y_0+1} \frac{1}{k \log k \cdot L(k)} < \int_{y_0}^{\infty} \frac{dt}{t \log t \cdot L(t)}$$

which converges; consequently, there is some nonnegative integer k_0 such that $\sum_{k>k_0} 1/q_k < 1/2$. Then the sequence $\{p_k\}$ defined by $p_k = q_{k_0+k}$ has the required properties. □

Proof of Theorem 1. Note that if $c > 0$ is fixed,

$$p_{\lfloor c \log_2 x \rfloor} \sim c \log_2 x \cdot \log_3 x \cdot L\big(c \log_2 x\big) \sim c \log_2 x \cdot \log_3 x \cdot L(\log_2 x)$$

by the slowly varying property of L. Applying this with $c = \frac{1}{2}$ and $c = \frac{3}{2}$, together with Proposition 6, proves Theorem 1. □

4. Proof of Theorem 2

For every positive integer j, define

$$\mathcal{A}_j = \big\{a \in \mathbb{N} \colon 2^{2^j} < a \le 2^{2^{j+1}},\ 2^j \parallel a\big\},$$

and define $\mathcal{A} = \bigcup_{j=1}^{\infty} \mathcal{A}_j$ (a disjoint union). It is clear that $A(x) \asymp x/\log x$, so that $\mathcal{A}$ has density 0 and the two assertions in (5) hold. It remains to show that if $\mathcal{S}$ is a primitive subset of $\mathcal{A}$, then (6) holds.

Let $\mathcal{S} \subset \mathcal{A}$ be primitive. For each natural number s, define s° to be the largest odd divisor of s, and define $\mathcal{S}^\circ = \{s^\circ \colon s \in \mathcal{S}\}$.

Lemma 9. *If $s_1, s_2 \in \mathcal{S}$ are distinct, then $s_1^\circ \nmid s_2^\circ$. In particular, $\mathcal{S}^\circ$ is also primitive, and the map $s \mapsto s^\circ$ is a bijection between $\mathcal{S}$ and $\mathcal{S}^\circ$.*

PROOF. Suppose, for the sake of contradiction, that $s_1^\circ \mid s_2^\circ$. Choose $j_1, j_2 \in \mathbb{N}$ so that $s_1 \in \mathcal{A}_{j_1}$ and $s_2 \in \mathcal{A}_{j_2}$. Since $s_1 = 2^{j_1} s_1^\circ$ and $s_2 = 2^{j_2} s_2^\circ$, the fact that $s_1 \nmid s_2$ (by primitivity of $\mathcal{S}$) forces $j_1 \geq j_2 + 1$. But then

$$s_1^\circ = \frac{s_1}{2^{j_1}} > 2^{2^{j_1} - j_1}$$

and

$$s_2^\circ = \frac{s_2}{2^{j_2}} \leq 2^{2^{j_2+1} - j_2} \leq 2^{2^{j_1} - (j_1 - 1)},$$

since the expression $2^k - (k-1)$ is an increasing function for $k \geq 1$. In particular, $s_2^\circ < 2s_1^\circ$, and so the divisibility relation $s_1^\circ \mid s_2^\circ$ forces $s_1^\circ = s_2^\circ$. But then $s_2 \mid s_1$, contradicting the primitivity of $\mathcal{S}$.

This shows that $s_1^\circ \nmid s_2^\circ$. The symmetric argument shows that $s_2^\circ \nmid s_1^\circ$, and so $\mathcal{S}^\circ$ is indeed primitive. Also, $s_1^\circ \nmid s_2^\circ$ implies that $s_1^\circ \neq s_2^\circ$, which shows that the map $s \mapsto s^\circ$ is a bijection between $\mathcal{S}$ and $\mathcal{S}^\circ$. □

If $s \in \mathcal{A}_j$ then $s^\circ = s/2^j$, and also $2^j \geq (\log s)/(2 \log 2)$ by the upper bound on elements of $\mathcal{A}_j$; these relations imply that

$$s^\circ \log s^\circ = \frac{s}{2^j} \log \frac{s}{2^j} \leq \frac{2s \log 2}{\log s} \log \frac{2s \log 2}{\log s} \ll s.$$

Therefore

$$\sum_{s \in \mathcal{S}} \frac{1}{s} \ll \sum_{s^\circ \in \mathcal{S}^\circ} \frac{1}{s^\circ \log s^\circ}$$

(using the injectivity of $s \mapsto s^\circ$). However, $\mathcal{S}^\circ$ is primitive, and so the last sum is convergent by (1). This proves (6).

References

[1] R. AHLSWEDE, L. H. KHACHATRIAN, AND A. SÁRKÖZY, On the counting function of primitive sets of integers, *J. Number Theory* **79** (1999), 330–344.

[2] A. S. BESICOVITCH, On the density of certain sequences of integers, *Math. Ann* **110** (1934), 336–341.

[3] P. ERDŐS, Note on sequences of integers no one of which is divisible by any other, *J. London Math. Soc.* **10** (1935), 126–128.

[4] P. ERDŐS AND J.-L. NICOLAS, Sur la fonction: nombre de facteurs premiers de N, *L'Enseignement mathématique* **27** (1981), 3–27.

[5] P. ERDŐS, A. SÁRKÖZY, AND E. SZEMERÉDI, On divisibility properties of sequences of integers, *Colloq. Soc. János Bolyai* **2** (1970), 35–49.

[6] H. HALBERSTAM AND K. F. ROTH, Sequences (2nd ed.), *Springer–Verlag, New York–Berlin*, 1983.

[7] F. Luca and C. Pomerance, Irreducible radical extensions and Euler-function chains, *Integers* **7** (2007), A25. (Also pp. 351–362 in *Combinatorial number theory*, Landman et al., eds., de Gruyter, Berlin, 2007.).

[8] H. L. Montgomery and R. C. Vaughan, Multiplicative number theory I. Classical theory, *Cambridge U. Press*, *Cambridge*, 2007.

[9] K. K. Norton, Estimates for partial sums of the exponential series, *J. Math. Anal. Appl.* **63** (1978), 265–296.

[10] C. Pomerance and A. Sárközy, Combinatorial number theory, Handbook of combinatorics, Vol. 1 and 2, R. L. Graham, et al. eds., *Elsevier*, *Amsterdam*, 1995, 967–1018.

[11] I. Z. Ruzsa, Erdős and the integers, *J. Number Theory* **79, no. 1** (1999), 115–163.

[12] Z. Zhang, On a problem of Erdős concerning primitive sequences, *Math. Comp.* **60** (1993), 827–834.

department of mathematics
university of british columbia
room 121, 1984 mathematics road
vancouver, bc, canada v6t 1z2

E-mail: gerg@math.ubc.ca
URL: http://www.math.ubc.ca/~gerg

department of mathematics
dartmouth college
hanover, nh 03755, usa

E-mail: carl.pomerance@dartmouth.edu
URL: http://www.math.dartmouth.edu/~carlp