The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: http://www.tandfonline.com/loi/uamm20

Light Subsets of ℕ with Dense Quotient Sets

Shawn Hedman & David Rose

To cite this article: Shawn Hedman & David Rose (2009) Light Subsets of ℕ with Dense Quotient Sets, The American Mathematical Monthly, 116:7, 635-641, DOI: 10.1080/00029890.2009.11920981

To link to this article: https://doi.org/10.1080/00029890.2009.11920981

Published online: 13 Dec 2017.

REFERENCES

1. P. Erdős, Beweis eines Satzes von Tschebyschef, *Acta Litt. Sci. Szeged* **5** (1932) 194–198; also available at `http://www.math-inst.hu/~p_erdos/1932-01.pdf`.
2. ———, Ramanujan and I, in *Number Theory, Madras 1987*, Lecture Notes in Mathematics, no. 1395, Springer, Berlin, 1989; also available at `http://www.iisc.ernet.in/academy/resonance/Mar1998/pdf/Mar1998Reflections.pdf`.
3. S. Finch, *Mathematical Constants*, Encyclopedia of Mathematics and Its Applications, vol. 94, Cambridge University Press, Cambridge, 2003.
4. S. Laishram, On a conjecture on Ramanujan primes, 2009 (preprint).
5. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Chelsea, New York, 1974; 3rd (corrected) reprint of 1st ed., Teubner, Leipzig, 1909.
6. W. J. LeVeque, *Fundamentals of Number Theory*, Dover, Mineola, NY, 1996; reprint of the 1st ed., Addison-Wesley, Reading, MA, 1977.
7. D. Ramakrishnan, Existence of Ramanujan primes for GL(3), in *Contributions to Automorphic Forms, Geometry, and Number Theory: A Volume in Honor of Joseph Shalika*, H. Hida, D. Ramakrishnan, and F. Shahidi, eds., The Johns Hopkins University Press, Baltimore, 2004, 711–718.
8. S. Ramanujan, A proof of Bertrand's postulate, *J. Indian Math. Soc.* **11** (1919) 181–182; also available at `http://www.imsc.res.in/~rao/ramanujan/CamUnivCpapers/Cpaper24/page1.htm`.
9. ———, *Collected Papers of Srinivasa Ramanujan*, G. H. Hardy, S. Aiyar, P. Venkatesvara, and B. M. Wilson, eds., commentary by B. C. Berndt, American Mathematical Society, Providence, RI, 2000.
10. P. Ribenboim, *The Book of Prime Number Records*, 2nd ed., Springer-Verlag, New York, 1989.
11. J. B. Rosser, The nth prime is greater than $n \ln n$, *Proc. London Math. Soc.* **45** (1938) 21–44.
12. J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962) 64–94.
13. ———, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, *Math. Comp.* **29** (1975) 243–269.
14. J. Sondow, Sequence A104272: Ramanujan primes (2005), in The On-Line Encyclopedia of Integer Sequences, N. J. A. Sloane, ed., available at `http://www.research.att.com/~njas/sequences/A104272`.
15. ———, Ramanujan prime—From MathWorld, A Wolfram Web Resource, E. W. Weisstein, ed., `http://mathworld.wolfram.com/RamanujanPrime.html`.

209 West 97th Street, New York, NY 10025
jsondow@alumni.princeton.edu

Light Subsets of $\mathbb{N}$ with Dense Quotient Sets

Shawn Hedman and David Rose

1. INTRODUCTION. Given a set S of natural numbers, we define the *quotient set* of S to be the set $Q(S) = \{\frac{a}{b} \colon a, b \in S\}$. Which sets of natural numbers have quotient sets that are dense in $\mathbb{R}^+$? This question was raised by D. Hobby and D. M. Silberger in [**2**], where they proved that the set of quotients of prime numbers is dense in $\mathbb{R}^+$. We say that S is *Q-dense* if $Q(S)$ is dense in $\mathbb{R}^+$. In particular, if $Q(S) = \mathbb{Q}^+$, we say that S is *Q-complete*. A set of natural numbers is called *Q-sparse* if it is not Q-dense. At the conclusion of [**2**], Hobby and Silberger remark that Q-denseness and Q-sparseness are "indubitably related to the number theoretic and probabilistic densities of a sequence of positive integers," such as the densities discussed in Chapter 11 of [**4**]. We investigate this claim.

We make the following initial observation regarding Q-denseness.

Proposition 1. *If $S \subset \mathbb{N}$ is Q-dense then so is $S \setminus F$ for any finite set F.*

Proof. By induction, it suffices to show that S_0 is Q-dense, where $S_0 = S \setminus \{a\}$ for fixed $a \in S$. Let $D = \{\frac{a}{b} : b \in S\} \bigcup \{\frac{b}{a} : b \in S\}$. The 'D' stands not for 'dense' but for 'discrete.' Because $0 \notin \mathbb{R}^+$, D is closed and discrete and hence nowhere dense in $\mathbb{R}^+$. Because $Q(S) = Q(S_0) \cup D$ is dense in $\mathbb{R}^+$, so is $Q(S_0)$. ■

It follows that the properties of Q-denseness and Q-sparseness are determined by the tail of the set S. It therefore seems reasonable to consider the density of the set as defined in Chapter 11 of [**4**]. For each $n \in \mathbb{N}$, let $S_n = \{s \in S : s \leq n\}$.

Definition 1. The *natural density* of S, denoted $\delta(S)$, is defined as:

$$\delta(S) = \lim_{n\to\infty} \frac{|S_n|}{n}.$$

The natural density measures the tenuousness of an infinite subset of $\mathbb{N}$. For example, if E is the set of even numbers, then $\delta(E) = \frac{1}{2}$. More generally, given $b, d \in \mathbb{N}$, the arithmetic progression $A_{(b,d)} = \{b + dn : n \in \mathbb{N}\}$ has natural density $\delta(A_{(b,d)}) = \frac{1}{d}$. We say that a set $S \subset \mathbb{N}$ is *light* if $\delta(S) = 0$. As we shall show, lightness is neither a necessary nor a sufficient condition for Q-sparseness.

2. EXTREMELY LIGHT SETS. We generalize the notion of lightness as follows.

Definition 2. Let $f : \mathbb{R}^+ \to \mathbb{R}^+$ be increasing and unbounded. A set $S \subset \mathbb{N}$ is *f-light* if $\lim_{n\to\infty} |S_n|/f(n) = 0$.

Definition 3. For each $p \in \mathbb{N}$, a set $S \subset \mathbb{N}$ is *p-light* if it is f-light for $f(x) = x^{1/p}$. So light sets are 1-light. If S is p-light for all p, then it is *ultra-light*.

In the examples and sections that follow, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x.

Example 1. For each $p \in \mathbb{N}$, the set $A(p) = \{n^{p+1} : n \in \mathbb{N}\}$ is p-light but not $(p+1)$-light. To see this, note that

$$\begin{aligned} 0 \leq \lim_{n\to\infty} \frac{|(A(p))_n|}{\sqrt[p]{n}} &= \lim_{n\to\infty} \frac{\lfloor \sqrt[p+1]{n} \rfloor}{\sqrt[p]{n}} \\ \leq \lim_{n\to\infty} \frac{\sqrt[p+1]{n}}{\sqrt[p]{n}} &= \lim_{n\to\infty} \frac{1}{\sqrt[p(p+1)]{n}} = 0, \end{aligned}$$

whereas $\left\langle |(A(p))_n| / \sqrt[p+1]{n} \right\rangle_{n=1}^{\infty}$ has the constant nonzero subsequence

$$\left\langle \frac{|(A(p))_{n^{p+1}}|}{\sqrt[p+1]{n^{p+1}}} \right\rangle_{n=1}^{\infty} = \langle 1 \rangle_{n=1}^{\infty}.$$

Example 2. For each $a > 1$, the set $B(a) = \{a^n : n \in \mathbb{N}\}$ is ultra-light but not ln-light. To see this, note that for each $p \in \mathbb{N}$,

$$\begin{aligned} 0 \leq \lim_{n\to\infty} \frac{|(B(a))_n|}{\sqrt[p]{n}} &= \lim_{n\to\infty} \frac{\lfloor \log_a n \rfloor}{\sqrt[p]{n}} \\ \leq \lim_{n\to\infty} \frac{\log_a n}{\sqrt[p]{n}} &= \left(\frac{p}{\ln a}\right) \lim_{n\to\infty} \frac{\ln \sqrt[p]{n}}{\sqrt[p]{n}} \end{aligned}$$

$$\leq \left(\frac{p}{\ln a}\right) \lim_{n\to\infty} \frac{1}{\sqrt[2p]{n}} = 0,$$

whereas

$$\lim_{n\to\infty} \frac{|B(a)_{a^n}|}{\ln a^n} = \lim_{n\to\infty} \frac{n}{n \ln a} = \frac{1}{\ln a} > 0.$$

Definition 4. For each $k \in \mathbb{N}$, a set $S \subset \mathbb{N}$ is *k-log-light* if it is f-light for

$$f(x) = \underbrace{\ln(\ln(\ldots(\ln}_{k \text{ times}}(x)))).$$

So ln-light sets are 1-log-light. If S is k-log-light for all k, then it is *ultra-log-light*.

Example 3. The set $C = \{n^n : n \in \mathbb{N}\}$ is 1-log-light but not 2-log-light. To see this, note that $|C_n|^{|C_n|} \leq n$ so that $|C_n| \ln |C_n| \leq \ln n$ for each $n \in \mathbb{N}$. We have

$$0 \leq \lim_{n\to\infty} \frac{|C_n|}{\ln n} \leq \lim_{n\to\infty} \frac{|C_n|}{|C_n| \ln |C_n|} = \lim_{n\to\infty} \frac{1}{\ln |C_n|} = 0.$$

On the other hand,

$$\lim_{n\to\infty} \frac{|C_{n^n}|}{\ln(\ln n^n)} = \lim_{n\to\infty} \frac{n}{\ln n + \ln(\ln n)} = \infty.$$

Similarly, for each $k \in \mathbb{N}$, the set

$$C(k) = \{\underbrace{n^{n^{\cdot^{\cdot^{\cdot^{n}}}}}}_{k+1 \text{ times}} : n \in \mathbb{N}\}$$

is k-log-light but not $(k+1)$-log-light.

Example 4. Consider the Ackermann function $\alpha : (\mathbb{N} \cup \{0\})^2 \to \mathbb{N}$ defined inductively by:

$$\alpha(0, x) = x + 1, \alpha(n+1, 0) = \alpha(n, 1), \text{ and } \alpha(n+1, x+1) = \alpha(n, \alpha(n+1, x)).$$

The function $g(n) = \alpha(n, n)$ grows faster than any primitive recursive function (see [**1**, Section 7.1.2]). It follows that the range of $g(n)$ (for $n \in \mathbb{N}$) is ultra-log-light.

Each set in Examples 1–4 is Q-sparse. In contrast, consider the set of primes. It follows from the prime number theorem that the primes are 1-light but not 2-light. Yet Hobby and Silberger demonstrated that the primes are Q-dense and therefore not Q-sparse. Recently, Syrous Marivani [**3**] has reportedly improved the Hobby-Silberger result by showing that the set of Dirichlet primes $P_{(a,b)}$ contained in the arithmetic sequence $a + b\mathbb{N}$, where $a, b \in \mathbb{N}$ are coprime, is Q-dense. Moreover, it follows from the prime number theorem for Dirchlet primes due to Vallee-Poussin [**5**] that $P_{(a,b)}$ is also light but not 2-light.

We now show that arbitrarily light Q-dense sets exist.

Theorem 1. *Let $f : \mathbb{R}^+ \to \mathbb{R}^+$ be increasing and unbounded. There exists a set $S \subset \mathbb{N}$ that is both f-light and Q-complete.*

Proof. Define $g : \mathbb{N} \to \mathbb{N}$ by $g(n) = y$ where y is the smallest natural number such that $f(y) > n^2$. Enumerate the positive rational numbers as $\mathbb{Q}^+ = \{q_i : i \in \mathbb{N}\}$. Construct the set $S = \{s_i : i \in \mathbb{N}\}$ by repeating the following step for each $n \in \mathbb{N}$: *Step n:* Choose s_{2n-1} and s_{2n} greater than $g(2n)$ with $s_{2n-1}/s_{2n} = q_n$.

The last condition entails $Q(S) = \mathbb{Q}^+$, and so S is Q-complete. The first condition entails that $s_n > g(n)$ for each n. Fix $n \in \mathbb{N}$. For each $s_i \in S_n$ we claim that $i \leq \sqrt{f(n)}$. Otherwise $f(n) < i^2$, which implies $g(i) > n$ (by the definition of g). But then we have $s_i > g(i) > n$, contradicting $s_i \in S_n$. It follows that $|S_n| \leq \sqrt{f(n)}$. We have:

$$\lim_{n\to\infty} \frac{|S_n|}{f(n)} \leq \lim_{n\to\infty} \frac{\sqrt{f(n)}}{f(n)} = \lim_{n\to\infty} \frac{1}{\sqrt{f(n)}} = 0$$

so that S is f-light as we wanted to show. ■

Corollary 1. *There exist ultra-log-light sets that are not Q-sparse.*

Proof. Let R be the range of $g(n)$ from Example 4 and let $f(x) = |\{y \in R : y < x\}|$. By Theorem 1, there exists $S \subset \mathbb{N}$ that is f-light and Q-dense. ■

3. RATIOS OF POWERS. Fix $a \in \mathbb{N}$ with $a > 1$ and recall the set $B(a) = \{a^n : n \in \mathbb{N}\}$ from Example 2. As was shown, $B(a)$ is ultra-light. Because $Q(B(a)) \cap (\frac{1}{a}, a) = \{1\}$, $B(a)$ is Q-sparse. Now fix $b \in \mathbb{N}$ with $b > 1$ and $\gcd(a, b) = 1$. Let $B(a, b) = B(a) \cup B(b)$. We prove that $Q(B(a, b))$ is dense in $\mathbb{R}^+$. This demonstrates that the union of two Q-sparse sets need not be Q-sparse. It also provides concrete examples of ultra-light sets that are not Q-sparse. We verify the Q-denseness of $B(a, b)$ in Section 3.2. We first establish a needed lemma.

3.1. Integer multiples of irrational numbers (mod 1). Let x be a real number. The fractional part of x is here denoted by $[x] = x - \lfloor x \rfloor$. We let D_x denote the set $\{[nx] : n \in \mathbb{N}\}$. Clearly, D_x is finite if x is rational. We prove that D_x is dense in $(0, 1)$ if x is irrational.

Proposition 2. *If x is irrational, then $[mx] \neq [nx]$ for distinct m and n in $\mathbb{N}$.*

Proof. $[mx] = [nx]$ implies $mx - nx = k$ for some integer k. But this implies $x = \frac{k}{m-n}$ contradicting the irrationality of x. ■

Proposition 3. *For $k \in \mathbb{N}$, $k[x] < 1$ implies $k[x] = [kx]$.*

Proof. If x is an integer, then $k[x] = [kx] = 0$. Otherwise, $k[x] < 1$ implies $0 < k(x - \lfloor x \rfloor) < 1$ which implies $k\lfloor x \rfloor < kx < k\lfloor x \rfloor + 1$. It follows that $\lfloor kx \rfloor = k\lfloor x \rfloor$. Now $k[x] = k(x - \lfloor x \rfloor) = kx - k\lfloor x \rfloor = kx - \lfloor kx \rfloor = [kx]$. ■

Lemma 1. *If x is irrational, then D_x is dense in $(0, 1)$.*

Proof. We show that $D_x \cap (u, v) \neq \emptyset$ whenever $0 < u < v < 1$. Take ϵ such that $0 < \epsilon < (v - u)$. The sequence $\{[nx]\}_{n=1}^{\infty}$ is bounded and therefore has a monotonic convergent subsequence. By Proposition 2, the terms of the sequence are distinct, and so this subsequence is either strictly increasing or strictly decreasing. Suppose first that $\{[nx]\}_{n=1}^{\infty}$ has a strictly increasing convergent subsequence. Then we can choose natural numbers $m < n$ such that

$$0 < [nx] - [mx] < \epsilon.$$

By definition of $[nx]$ and $[mx]$:

$$0 < (nx - \lfloor nx \rfloor) - (mx - \lfloor mx \rfloor) < \epsilon$$
$$0 < (n-m)x - (\lfloor nx \rfloor - \lfloor mx \rfloor) < \epsilon$$
$$(\lfloor nx \rfloor - \lfloor mx \rfloor) < (n-m)x < (\lfloor nx \rfloor - \lfloor mx \rfloor) + \epsilon.$$

Because $\epsilon < (v-u) < 1$, $(n-m)x$ is between the consecutive integers $(\lfloor nx \rfloor - \lfloor mx \rfloor)$ and $(\lfloor nx \rfloor - \lfloor mx \rfloor) + 1$. Thus $\lfloor (n-m)x \rfloor = (\lfloor nx \rfloor - \lfloor mx \rfloor)$, and so we have:

$$\begin{aligned} 0 < [(n-m)x] &= (n-m)x - \lfloor (n-m)x \rfloor \\ &= (n-m)x - (\lfloor nx \rfloor - \lfloor mx \rfloor) \\ &= [nx] - [mx] < \epsilon. \end{aligned}$$

Because $\epsilon < (v-u)$, there exists an integer $k > 0$ so that $u < k[(n-m)x] < v$. By Proposition 3, $k[(n-m)x] = [k(n-m)x]$. We have $[k(n-m)x] \in D_x \cap (u, v)$ as we wanted to show.

Now suppose that the monotonic convergent subsequence of $\{[nx]\}_{n=1}^{\infty}$ is strictly decreasing. Then the same argument shows that D_{-x} is dense in $(0, 1)$. But D_{-x} is the image of D_x under the homeomorphism $x \mapsto 1 - x$. Since D_{-x} is dense in $(0, 1)$, so is D_x. ■

Corollary 2. *For irrational x and $N \in \mathbb{N}$, the set $D_{(x,N)} = \{[nx] : n > N\}$ is dense in* $(0, 1)$.

Proof. This follows from Lemma 1 and the fact that $D_x \setminus D_{(x,N)}$ is finite. ■

3.2. $B(a, b)$ is not Q-sparse for co-prime a and b.

Theorem 2. *If* $\gcd(a, b) = 1$ *and* $a > 1$ *and* $b > 1$*, then $Q(B(a, b))$ is dense in $\mathbb{R}^+$.*

Proof. Let $x = \log_a(b)$. This is an irrational number. Otherwise, if $x = \frac{n}{m}$ for $m, n \in \mathbb{N}$, then $a^n = b^m$. This contradicts $\gcd(a, b) = 1$.

Let $L = \{nx - m : m, n \in \mathbb{N}\}$. Because $a^{nx-m} = b^n/a^m$, the image of L under the homeomorphism $x \mapsto a^x$ is a proper subset of $Q(B(a, b))$. So to show that $Q(B(a, b))$ is dense in $\mathbb{R}^+$, it suffices to show that L is dense in $\mathbb{R}$.

Fix r and ϵ in $\mathbb{R}$ with $\epsilon > 0$. To show that L is dense in $\mathbb{R}$, it suffices to find $m, n \in \mathbb{N}$ with $|(nx - m) - r| < \epsilon$.

Fix $N \in \mathbb{N}$ so that $N > \frac{r+1}{x}$. By Corollary 2, the set $D_{(x,N)} = \{[nx] : n > N\}$ is dense in $(0, 1)$. So there exists $n > N$ so that $|[nx] - [r]| < \epsilon$. We have $|(nx - \lfloor nx \rfloor) - (r - \lfloor r \rfloor)| < \epsilon$ and so $|nx - (\lfloor nx \rfloor - \lfloor r \rfloor) - r| < \epsilon$.

Let $m = (\lfloor nx \rfloor - \lfloor r \rfloor)$. Because $n > \frac{r+1}{x}$, we have $m \geq 1$. Now $(nx - m) \in L$ and $|(nx - m) - r| < \epsilon$ as we wanted to show. ■

Corollary 3. *The natural numbers can be partitioned as $\mathbb{N} = \sqcup_{i=1}^{\infty} N_i$ where each N_i is Q-dense and $Q(N_i) \cap Q(N_j) = \emptyset$ for $i \neq j$.*

Proof. Let $N_1 = B(2, 3) \cup \{1\}$. For $i > 1$, let $N_i = B(a_i, b_i)$, where a_i is least such that $a_i \notin N_j$ for $j < i$ and b_i is such that $\gcd(a_i, b_i) = 1$ and $b_i \notin N_j$ for $j < i$. ■

4. NON-LIGHT SETS. If a set $S \subset \mathbb{N}$ is not light, then either $\lim_{n\to\infty} |S_n|/n > 0$ or else this limit does not exist. We show that S is necessarily Q-dense in the first case but not the second.

Proposition 4. *If $\delta(S) = \ell > 0$, then $Q(S)$ is dense in $\mathbb{R}^+$.*

Proof. Fix $q \in \mathbb{Q}^+$ and $\epsilon > 0$. Enumerate S as an increasing sequence $\langle s_i : i \in \mathbb{N}\rangle$. It suffices to find $s_n, s_m \in S$ with $|\frac{s_m}{s_n} - q| < \epsilon$.

According to Theorem 11.1 of [**4**], $\lim_{n\to\infty} n/s_n = \lim_{n\to\infty} |S_n|/n = \ell$. Since $\ell > 0$, there exists N so that $n, m > N$ implies

$$\left|\frac{(n/s_n)}{(m/s_m)} - 1\right| < \frac{\epsilon}{q}.$$

Choose $n, m > N$ so that $m/n = q$. We have:

$$\left|\frac{n}{s_n}\frac{s_m}{m} - 1\right| = \left|\frac{s_m/s_n}{q} - 1\right| < \frac{\epsilon}{q}$$

which implies $|s_m/s_n - q| < \epsilon$. ■

Proposition 5. *There exists a non-light Q-sparse set.*

Proof. Consider $S = \mathbb{N} \cap \left(\bigcup_{n=1}^{\infty} [2^{3n-1}, 2^{3n}]\right)$. The first several terms of this set are

$$4, 5, 6, 7, 8, 32, 33, \ldots, 63, 64, 256, 257, \ldots, 511, 512, 2048, 2049, \ldots$$

To see that S is Q-sparse, take $p, q \in S$ with $p < q$. If $\{p, q\} \subset [2^{3n-1}, 2^{3n}]$ for some $n \in \mathbb{N}$, then $q/p \leq 2^{3n}/2^{3n-1} = 2$. Otherwise, $p \in [2^{3n-1}, 2^{3n}]$ and $q \in [2^{3m-1}, 2^{3m}]$ for some $m, n \in \mathbb{N}$ with $m < n$. In this case, $q/p \geq 2^{3n-1}/2^{3m} \geq 2^{3n-1}/2^{3(n-1)} = 4$. It follows that $S \cap (2, 4) = \emptyset$ and S is Q-sparse as claimed.

To show that S is not light, it suffices to show that a subsequence of $\langle |S_n|/n\rangle_{n=1}^{+\infty}$ has a positive limit. Indeed,

$$\begin{aligned}
\lim_{n\to\infty} \frac{|S_{2^{3n}}|}{2^{3n}} &= \lim_{n\to\infty} \frac{n + \sum_{k=0}^{n-1} 2^{3(n-k)-1}}{2^{3n}} \\
&= \lim_{n\to\infty} \frac{\sum_{k=0}^{n-1} 2^{3(n-k)-1}}{2^{3n}} \\
&= \frac{1}{2} \lim_{n\to\infty} \sum_{k=0}^{n-1} \left(\frac{1}{8}\right)^k \\
&= \frac{1}{2} \sum_{k=0}^{\infty} \left(\frac{1}{8}\right)^k = \frac{4}{7} > 0.
\end{aligned}$$

■

5. CONCLUSION. The Q-sparseness of a set of natural numbers does not depend on the natural density of the set. The set S in the proof of Proposition 5 contains arbitrarily long sequences of consecutive integers and is Q-sparse. On the other hand, according to Corollary 1 there exist ultra-log-light sets that are not Q-sparse.

REFERENCES

1. S. Hedman, *A First Course in Logic*, Oxford University Press, New York, 2004.
2. D. Hobby and D. M. Silberger, Quotients of Primes, this MONTHLY **100** (1993) 50–52.
3. S. Marivani, On some particular dense sets, talk at the spring 2008 Southeastern Regional AMS meeting, Baton Rouge, LA.
4. I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, New York, 1991.
5. J. E. Shockley, *Introduction to Number Theory*, Holt, Rinehart and Winston, New York, 1967.

Department of Mathematics and Computer Science, Florida Southern College, Lakeland, FL 33801
shedman@flsouthern.edu
drose@flsouthern.edu

The Least Prime in Certain Arithmetic Progressions

Juan Sabia and Susana Tesauri

Dirichlet's theorem states that, if a and n are relatively prime integers, there are infinitely many primes in the arithmetic progression $n + a$, $2n + a$, $3n + a$, ... However, as stated in [**3**], the known proofs of this general result are not elementary (see [**1, 10, 12**], for example). Linnik [**4, 5**] proved that, if $1 \le a < n$, there are absolute constants c_1 and c_2 so that the least prime p in such a progression satisfies $p \le c_1 n^{c_2}$, but his proof is not elementary either. There are several different proofs of Dirichlet's theorem for the particular case $a = 1$ (see for example [**2, 6, 9, 11**]). In [**7**], moreover, the bound $p < n^{3n}$ for the least prime satisfying $p \equiv 1 \pmod n$ is given.

Our aim is to use an elementary argument, which also shows that there are infinitely many primes $\equiv 1 \pmod n$, to prove that the least such prime lies below $(3^n - 1)/2$.

For $n = 2$, the result is obvious, so let n be an integer, $n > 2$. Let $\Phi_n(x)$ denote the nth cyclotomic polynomial. That is,

$$\Phi_n(x) = \prod_{\substack{a=1 \\ (a,n)=1}}^{n} \left(x - e^{2\pi i a/n}\right)$$

is the polynomial of degree $\phi(n)$ whose zeros are the primitive nth roots of unity. It is well known that $\Phi_n(x)$ is a monic, irreducible polynomial with integer coefficients.

Our proof is based on the following observation: For any integer b, the prime factors of $\Phi_n(b)$ are either prime divisors of n, or are $\equiv 1 \pmod n$. Moreover, if $n > 2$, any prime divisor of n can divide $\Phi_n(b)$ only to the exponent 1; that is, its square does not divide $\Phi_n(b)$.