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, the known proofs of this general result are not elementary (see [**1, 10, 12**], for example). Linnik [**4, 5**] proved that, if $1 \leq a < n$, there are absolute constants c_1 and c_2 so that the least prime p in such a progression satisfies $p \leq c_1 n^{c_2}$, 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 $\Phi_n(b)$.

Granting the observation, let us prove that the least prime $\equiv 1 \pmod{n}$ is $\leq (3^n - 1)/2$. Note that $\Phi_n(3)$ is an integer whose absolute value is

$$|\Phi_n(3)| = \prod_{\substack{a=1\\(a,n)=1}}^{n} \left|3 - e^{2\pi i a/n}\right| > 2^{\phi(n)} \geq \prod_{q|n} q,$$

where the product above is over the distinct primes dividing n, and the final inequality follows because $\phi(n) \geq \sum_{q|n}(q-1)$ and $2^{q-1} \geq q$. From our observation and this lower bound, it follows that $\Phi_n(3)$ must be divisible by some prime not dividing n, and that prime is necessarily $\equiv 1 \pmod{n}$. Finally, $\Phi_n(3)$ divides $(3^n-1)/(3-1)$, and so we know that there is some prime $\equiv 1 \pmod{n}$ below $(3^n-1)/2$.

This same argument can be used to prove there are infinitely many primes $\equiv 1 \pmod{n}$: Suppose $p_1, \dots, p_r$ are such primes; then $\Phi_n(\prod_{i=1}^r p_i)$ is relatively prime to $\prod_{i=1}^r p_i$, so any prime $\equiv 1 \pmod{n}$ in the factorization of $\Phi_n(\prod_{i=1}^r p_i)$ must be different from $p_1, \dots, p_r$.

We now prove our observation. Suppose $p \mid \Phi_n(b)$, and so $p \mid (b^n - 1)$. Thus the order of $b \pmod{p}$ is a divisor of n. If it is exactly n then, since the order has to divide $p-1$, we have $p \equiv 1 \pmod{n}$, as desired.

Suppose that the order is not exactly n. In this case, for some prime divisor q of n we must have $p \mid (b^{n/q} - 1)$. The cyclotomic polynomial $\Phi_n(x)$ divides $(x^n-1)/(x^{n/q}-1) = 1 + x^{n/q} + \cdots + x^{n(q-1)/q}$. By Gauss's Lemma the quotient is a polynomial with integer coefficients. Thus $\Phi_n(b)$ divides $(b^n-1)/(b^{n/q}-1) = 1 + b^{n/q} + \cdots + b^{n(q-1)/q}$. Now by assumption $b^{n/q} \equiv 1 \pmod{p}$, and so $(b^n-1)/(b^{n/q}-1) \equiv q \pmod{p}$; however $(b^n-1)/(b^{n/q}-1)$ is also a multiple of $\Phi_n(b)$ which is a multiple of p. Therefore we have $q \equiv 0 \pmod{p}$, or in other words $p = q$ is a divisor of n.

It remains lastly to show that if q is a prime divisor of $n > 2$, and $q \mid \Phi_n(b)$ for some b, then $q^2 \nmid \Phi_n(b)$. From our argument above we know that $b^{n/q} = 1 + cq$ for some integer c, and using the binomial theorem $b^{nj/q} \equiv 1 + cjq \pmod{q^2}$ so that

$$\frac{b^n - 1}{b^{n/q} - 1} = 1 + b^{n/q} + \cdots + b^{n(q-1)/q} \equiv q + cq\frac{q(q-1)}{2} \pmod{q^2}.$$

If q is odd then the above is $\equiv q \pmod{q^2}$ and therefore q^2 cannot divide $\Phi_n(b)$. If $q = 2$ then the above is $\equiv 2(1+c) \pmod{4}$, and we are done unless c is odd. In that case $b^{n/2} \equiv 3 \pmod{4}$, from which it follows that b and $n/2$ are odd. But if $n/2$ is odd then $\Phi_n(b)$ is a divisor of $\sum_{i=0}^{n/2-1}(-b)^i$, which is odd, and thus this last case cannot arise.

The observation that we have used in our proof is quite old: according to Ribenboim [**8**], variants of this were shown by Legendre in 1830. In terms of algebraic number theory, it is simply the fact that the non-inert primes in the nth cyclotomic field are the primes dividing n (which ramify), and the primes that are $\equiv 1 \pmod{n}$ (which split completely).

REFERENCES

1. G. L. Dirichlet, *Dirichlet's Werke*, G. Reimer, Berlin, 1889.
2. T. Estermann, Note on a paper of A. Rotkiewicz, *Acta Arith.* **8** (1963) 465–467.
3. G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Clarendon Press, Oxford, 1960.
4. U. V. Linnik, On the least prime in an arithmetic progression. I. The basic theorem, *Rec. Math. (Mat. Sb.) N. S.* **15** (1944) 139–178.

5. ———, On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon, *Rec. Math. (Mat. Sb.) N. S.* **15** (1944) 347–368.
6. T. Nagell, *Introduction to Number Theory*, Wiley, New York, 1951.
7. I. Niven and B. Powell, Primes in certain arithmetic progressions, this MONTHLY **83** (1976) 467–469.
8. P. Ribenboim, *The Book of Prime Number Records*, Springer-Verlag, New York, 1988.
9. A. Rotkiewicz, Démonstration arithmétique de l'existence d'une infinité de nombres premiers de la forme $nk + 1$, *Enseign. Math.* **7** (1962) 277–280.
10. A. Selberg, An elementary proof of Dirichlet's theorem about primes in an arithmetic progression, *Ann. Math.* **50** (1949) 297–304.
11. W. Sierpinski, *Elementary Theory of Numbers*, Hafner, New York, 1964.
12. H. Zassenhaus, Über die Existenz von Primzahlen in arithmetischen Progressionen, *Comment. Math. Helv.* **22** (1949) 232–259.

Departamento de Matemática, FCEyN - Departamento de Cs. Exactas, CBC,
Universidad de Buenos Aires–Ciudad Universitaria–Pabellón I, 1428 Buenos Aires, Argentina
jsabia@dm.uba.ar
stesauri@dm.uba.ar

A Simple Continuous Bijection from Natural Sequences to Dyadic Sequences

Oliver Deiser

1. INTRODUCTION. Surprising bijections have been constructed between spaces thought to be too different in nature to allow one-to-one correspondences. In his seminal paper of 1878, Georg Cantor constructed a bijection between the real line $\mathbb{R}$ and the plane $\mathbb{R}^2$, revealing the intuition of "two variables" as too crude to define the notion of dimension. The lack of continuity of Cantor's mapping was noted immediately by Richard Dedekind, but continuous counter-intuitive results were found, too: in 1890 Giuseppe Peano and David Hilbert constructed continuous surjections from the closed real unit interval $I = [0, 1]$ to I^2, now known as Peano curves. But Peano curves lack injectivity, and finally Luitzen Brouwer showed in 1911 that they have to: there is no continuous bijection between $\mathbb{R}^n$ and $\mathbb{R}^m$ (or I^n and I^m) whenever $n \neq m$. Brouwer's proof uses special topological properties of the continuum. In the 1920s, Karl Menger, Pavel Urysohn and others developed a general theory of topological dimension. The reader might consult [**3**], [**4**], or [**6**] for the history of the many different paths originating from Cantor's initial discovery. Spanning half a century, this single topic interestingly mirrors the development of modern mathematics.

In contrast to Brouwer's result, there are many continuous bijections if we switch from the "analog" reals $\mathbb{R}$ to the "digital" Baire space $\mathcal{N}$ consisting of all infinite sequences of natural numbers, equipped with the infinite product topology of the discrete topology on $\mathbb{N}$. $\mathcal{N}$ is homeomorphic to the irrational numbers via continued fractions. It is easy to see that $\mathcal{N}$ is homeomorphic to $\mathcal{N}^n$ for all $n \geq 1$, and $\mathcal{N}$ is even homeomorphic to $\mathcal{N}^{\mathbb{N}}$. Moreover, Wacław Sierpiński proved in 1929 a remarkable theorem, which in its modern general form reads: if X is any nonempty perfect Polish space, then there is a continuous bijection from $\mathcal{N}$ to X. (See [**7**, pp. 40, 357]. A *Polish space* is a topological space which has a countable dense subset and which is complete with respect to a metric generating the topology. A space is *perfect* if it has no isolated