Adic Topologies for the Rational Integers

Version:7th June 2002

Kevin A. Broughan

University of Waikato, Hamilton, New Zealand
E-mail: kab@waikato.ac.nz

A topology on $\mathbb{Z}$, which gives a nice proof that the set of prime integers is infinite, is characterised and examined. It is found to be homeomorphic to $\mathbb{Q}$, with a compact completion homeomorphic to the Cantor set. It has a natural place in a family of topologies on $\mathbb{Z}$, which includes the p-adics, and one in which the set of rational primes $\mathbb{P}$ is dense. Examples from number theory are given, including the primes and squares, Fermat numbers, Fibonacci numbers and k-free numbers.

Key Words: p-adic, metrizable, quasi-valuation, topological ring, completion, inverse limit, diophantine equation, prime integers, Fermat numbers, Fibonnaci numbers.

MSC2000 11B05, 11B25, 11B50, 13J10, 13B35.

1. INTRODUCTION

There is a nice topology on $\mathbb{Z}$, highlighted in reference [2], which enables a very elegant proof to be given that the number of rational primes is infinite. In this paper we develop properties of this topology, define a class of metrics which generate it, establish a natural family of topologies (the adic topologies) of which this is the finest and which includes the p-adic topologies, and give some examples from number theory.

The motivation behind this work is to provide some tools which will assist with the description and comparison of sets of integers, which are of number theoretic interest.

2. TOPOLOGIES FOR $\mathbb{Z}$

Definition of $(\mathbb{Z}, \tau)$: for each $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ with $b \geq 1$, let

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$$

Then for each a and $b_1 \geq 1$, $b_2 \geq 1$

$$N_{a,b_1 b_2} \subset N_{a,b_1} \cap N_{a,b_2}$$

so the family $(N_{a,b})$ is a base for the neighbourhoods of each point a and generates a topology, τ on $\mathbb{Z}$, called here the full topology.

Now generalize this idea. For each $a \in \mathbb{Z}$ let G_a be a multiplicative sub-semigroup of $\mathbb{N}$ with 1 and let $\mathcal{G} = (G_a : a \in \mathbb{Z})$. Then let $\tau_{\mathcal{G}}$ be the topology on $\mathbb{Z}$ generated by $\mathcal{B} = (N_{a,b} : a \in \mathbb{Z}, b \in G_a)$, which is a sub-base.

If $\mathcal{G} \subset \mathcal{G}'$ then $\tau_{\mathcal{G}} \subset \tau_{\mathcal{G}'}$. Therefore $\tau_{\mathcal{G}} \subset \tau$ for all families $\mathcal{G}$. Therefore, in this class of topologies on $\mathbb{Z}$, the topology τ, with $G_a = \mathbb{N}$ for all a, is the finest. Hence the designation "full" topology for τ.

We call topologies in this family "adic" topologies.

Example 2.1. If $G_a = \{1\}$ for each a, we obtain the indiscrete topology. In what follows, by the term semigroup we mean a sub multiplicative semigroup of $\mathbb{N}$ with 1 which, unless otherwise stated, is non-trivial in that it contains an element $b > 1$.

Example 2.2. Let p be a rational prime and, for each $a \in \mathbb{Z}$, let G_a be the semigroup generated by p, i.e. $G_a = \{p^n : n = 0, 1, 2, \cdots\}$. Then $\tau_{\mathcal{G}}$ is the classical p-adic topology.

Example 2.3. Examples where the semigroup G_a depends on a would include the semigroup generated by the prime divisors of a, by the maximal prime powers dividing a, by the powers of a, and by the multiples of a (with in each case special definitions being made for special values like $a = 0$).

All adic topologies make the multiplication $\cdot$ continuous.

Definition 2.1. If $G_a = G$ is independent of $a \in \mathbb{Z}$, we say $\tau_{\mathcal{G}}$ is flat and write τ_G instead of $\tau_{\mathcal{G}}$.

Definition 2.2. We say the semigroup G is divisor dense if for all $n \in \mathbb{N}$ there is a $b \in G$ such that $n \mid b$. If each G_a is divisor dense we say $\mathcal{G}$ is divisor dense.

Definition 2.3. If the semigroup G is such that $a \in G$ and $b \mid a$ implies $b \in G$ we say G is divisor complete. This is equivalent to G being generated by its prime elements. If each G_a is divisor complete we say $\mathcal{G}$ is divisor complete.

Flat topologies make addition $+$ continuous. If $\mathcal{G}$ is divisor dense, then $\mathcal{B}$ is a base for $\tau_{\mathcal{G}}$.

The semigroup collection $\mathcal{G}$ which generates the topology τ_m is neither divisor complete nor flat. However the corresponding $\mathcal{B}$ is still a base. To see this let $m > 1$ and let $x \in N_{a,b} \cap N_{a',b'} = N_{x,b} \cap N_{x,b'}$. Let $(x,b) = m^r$ and $(x,b') = m^{r'}$. There are positive integers r, r' such that $\beta m^r = b$ and $\beta' m^{r'} = b'$. Therefore $(\frac{x}{m^r}, \beta) = 1$, $(\frac{x}{m^{r'}}, \beta') = 1$ so if $r' \geq r$, $(\frac{x}{m^{r'}}, \beta\beta') = 1$ and hence, if $c = \beta\beta' m^{r'}$, $(x,c) = m^{r'}$. But c is a common multiple of b and b' and $N_{x,c} \in \mathcal{B}$. Hence $\mathcal{B}$ is a base.

Theorem 2.1. *If the shift maps $f_{\pm}(n) = n \pm 1$ are continuous and $\mathcal{G}$ divisor complete, then $\mathcal{G}$ is flat.*

Proof. If $b \in G_a$ then $f_{\pm}^{-1}(N_{a,b})$ is open so there is a b' with $b \mid b'$ such that $b' \in G_{a+1}$. But this implies $b \in G_{a+1}$ so $G_a \subset G_{a+1}$. Using the left shift we obtain the reverse implication, so $G_a = G_{a+1}$. Since this holds for all a, $\mathcal{G}$ is flat. ∎

If $m = 1$ so $G_a = \{b \geq 1 : (a,b) = 1\}$ we generate the so-called coprime topology τ_1. Note that in this case, each $\mathcal{G}$ is divisor complete.

Theorem 2.2. *The space $(\mathbb{Z} - \{0\}, \tau_1)$ is T_2, second countable, non-compact space, with no isolated points.*

Proof. The topology is T_2: If $x < y$ let p be a prime number with $y - x < p$. Then $N_{x,p} \cap N_{y,p} = \emptyset$ since, if not, $y - x = np$ for some integer n, which is impossible. It is second countable, being a first countable topology on a countable set. Since, for all primes p:

$$\mathbb{Z} \setminus N_{0,p} = \bigcup_{a=1}^{p-1} N_{a,p}$$

and each $(a,p) = 1$ when $1 \leq a \leq p-1$, each $N_{0,p}$ is closed in the coprime topology. If (p_i) is an enumeration of all primes, (N_{0,p_i}) has the finite intersection property, with empty intersection. Hence τ_1 is not compact. There are no isolated points since the topology is weaker than the full topology. ∎

Note that $G_0 = \{1\}$ and $N_{0,1} = \mathbb{Z}$, so $\mathbb{Z}$ is the only open set containing 0 and $(\mathbb{Z}, \tau_1)$ fails to be T_1.

Example 2.4. In the coprime topology the set of prime integers is dense, i.e. $\overline{\mathbb{P}} = \mathbb{Z}$. This follows directly from Dirichlet's theorem [1]. Indeed the result $\overline{\mathbb{P}} = \mathbb{Z}$ in τ_1 is equivalent to Dirichlet's theorem.

Theorem 2.3. *The space $(\mathbb{Z}, \tau_G)$ is T_1, first countable and makes $\mathbb{Z}$ a topological ring in which the usual operations are continuous. It is also metrizable and has* $\mathrm{Ind}(\mathbb{Z}) = 0$.

Proof. 1. τ_G is T_1: Given x and y in $\mathbb{Z}$ with $x \neq y$ let b be an element of $G_x = G$ with $b > x - y$. (Such an element exists because of the assumption $G \neq \{1\}$.) Then $y \notin N_{x,b}$.

2. $\mathbb{Z}$ is first countable: $(N_{a,b} : b \in G)$ is a countable base for the neighbourhoods of a.

3. $\mathbb{Z}$ is a topological ring: This follows directly because, for all x and $y \in \mathbb{Z}$ and $b \in G$:

$$N_{x,b} + N_{y,b} \subset N_{x+y,b} \text{ and } N_{x,b} \cdot N_{y,b} \subset N_{xy,b}.$$

4. Since $\mathbb{Z}$ is countable and first countable, it is second countable. Since, for every $b \in G$

$$\mathbb{Z} = \bigcup_{0 \le a < b} N_{a,b}$$

and the union is disjoint, each $N_{a,b}$ is closed as well as open. Therefore the topology has small inductive dimension zero and is T_2. Therefore [3] $\mathrm{Ind}(\mathbb{Z}) = 0$, so the space is also normal. Hence by Urysohn's metrization theorem, the topology is metrizable. ▮

Theorem 2.4. *The space $(\mathbb{Z}, \tau_G)$ is homeomorphic to $\mathbb{Q}$ with its usual topology.*

Proof. By the theorem of Sierpinski [9], the rationals are characterized topologically by the properties metric, countable and having no isolated points. The only property to prove is the last, which follows immediately because every non-empty open subset of τ_G contains a set $N_{a,b}$ so is infinite. ▮

3. COMPLETIONS

A non-archimedean quasi-valuation on a ring R is a function $v : R \to [0, \infty)$ such that, for all a and b in R:

(1) $v(0) = 0$,
(2) $v(a) > 0$ for $a \neq 0$,
(3) $v(a + b) \leq \max\{v(a), v(b)\}$,
(4) $v(ab) \leq \min\{v(a), v(b)\}$.

A pseudo-valuation has (4) replaced by $v(ab) \leq \max\{v(a), v(b)\}$ and a valuation by $v(ab) = v(a)v(b)$,[5].

Below we will refer to a non-archimedean quasi-valuation as simply a valuation.

Note that if $a \mid b$ then $v(b) \leq v(a)$ and that for each strictly positive real number δ, $\{x \in R | v(x) \leq \delta\}$ is a closed ideal in R in the topology induced by v.

Construction of the completion of a ring with a quasi-valuation proceeds in the normal manner, [5].

Let G be a semigroup. Define a particular quasi-valuation on $\mathbb{Z}$ as follows: let $1 = n_0 < n_1 < n_2$ be a strictly increasing sequence of elements of G with $n_1 | n_2 | n_3 \cdots$ and such that for all $i \in G$ there is a j such that $i | n_j$. For example, $G = \mathbb{N},\ n_i = i!$.

If $a = 0$ let $v(a) = 0$. Otherwise let $\langle a \rangle = \max\{n_i : n_i | a\}$ and then set $v(a) = 1/\langle a \rangle$.

Theorem 3.1. *The function v is a non-archimedean quasi-valuation on $\mathbb{Z}$ such that the associated metric $d(x, y) = v(x - y)$ generates the topology $\tau_{\mathcal{G}}$.*

Proof. Since both topologies are homogeneous we need only consider neighbourhoods of 0. Because $B(0, 1/n_j] = n_j\mathbb{Z}$, each $B(0, 1/n_j]$ is open in τ. Conversely, given $i \in G$ there is a j with $i \mid n_j \mid n_{j+1}$ and therefore

$$B(0, \frac{1}{n_j}) = N_{0,n_{j+1}} \subset N_{0,i}.$$

∎

Definition 3.1. Let G be a semigroup. We say a sequence (x_n) of integers is G-Cauchy if for all $i \in G$ there is an N_i such that for all $n, m \geq N_i$, $i \mid x_n - x_m$. By Cauchy we mean $\mathbb{N}$-Cauchy.

Definition 3.2. If (x_n) and (y_n) are two G-Cauchy sequences we say they are equivalent if for all $i \in G$ there is an N_i such that for all $n \geq N_i$, $i \mid x_n - y_n$.

Definition 3.3. If (x_n) is a sequence of integers and x_o an integer we say (x_n) converges to x_o if for all $i \in G$ there is an N_i such that for all $n \geq N_i$, $i \mid x_n - x_o$. When this is so we write $x_n \to x_o$.

Example 3.1. Let (α_i) be any sequence of integers and for each $n \in \mathbb{N}$ let $x_n = \sum_{j=1}^{n} j!\alpha_j$. Then (x_n) is Cauchy.

Definition 3.4. If G is a semigroup, $\mathbb{Z}^G$ is the completion of $\mathbb{Z}$ with respect to the valuation v_G.

Theorem 3.2. *The ring $\mathbb{Z}^G$ can be identified with (1) the set of equivalence classes of G-Cauchy sequences, with (2) the completion of $(\mathbb{Z}, \tau_G)$ as a topological ring, with (3) the inverse limit*

$$\mathbb{Z}^G \approx \lim_{\substack{\longleftarrow \\ b \in G}} \mathbb{Z}/b\mathbb{Z},$$

and, if G is divisor complete, with (4)

$$\mathbb{Z}^G \approx \prod_{p \in G} \mathbb{Z}_p$$

where the product is of rings of p-adic integers, one for each rational prime p in G.

Proof. (1) Let (x_n) be G-Cauchy. Given $b = n_i \in G$ there is an $N_b \in \mathbb{N}$ such that $b \mid x_n - x_m$ for all $n, m \geq N_b$. Then $v(b) \geq v(x_n - x_m)$. But $< b >= n_i$ which can be made arbitrarily large. Hence (x_n) is v-Cauchy.

Conversely, given $N \in \mathbb{N}$, let (x_n) be such that $v(x_n - x_m) < 1/N$ for all sufficiently large n, m. Then $< x_n - x_m >\geq N$ so there is an n_i with $n_i \geq N$ and $n_i \mid x_n - x_m$. The result now follows because given $b \in G$ we can chose N so $b \mid n_i$.

(2)This follows directly from (1) since v_G induces the topology τ_G on $\mathbb{Z}$.

(3)If (x_n) is a G-Cauchy sequence in $\mathbb{Z}$ and $b \in G$ is given, then for all n,m sufficiently large, $x_n \equiv x_m \mod b$. So each sequence maps to a well defined class in $\mathbb{Z}/b\mathbb{Z}$. It is easy to see that this map is independent of the representative for each element of the completion $\mathbb{Z}^G$ and that these maps commute with the natural surjections $\mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/c\mathbb{Z}$ when $b \mid c$. Hence the completion may be identified with the inverse limit

$$\mathbb{Z}^G \approx \varprojlim_{b \in G} \mathbb{Z}/b\mathbb{Z},$$

with the ordering for the limit being induced by divisibility.

(4) The given inverse limit can be specified with a compatible system of residue representatives (x_b), i.e. such at $x_m \equiv x_n \mod m$ whenever $m \mid n$. To specify an element of Z_p, a similar compatible system (x_{p^n}) must be given. If G is divisor complete, then all prime powers appear and the identification follows as an application of the ring theoretic version of the Chinese Remainder Theorem. ▮

Corollary 3.1. *The space $\mathbb{Z}^G$, is homeomorphic to the Cantor set $\{0,1\}^{\aleph_0}$.*

Proof. Since v_G gives rise to a non-archimedean metric, the completion also is non-archimedean, so is totally disconnected. It is also totally bounded since $\mathbb{Z}$ is a dense totally bounded subset. Hence the completion is metric and compact. It is also infinite and has no isolated point, since the same is true of $\mathbb{Z}$. These properties characterise the Cantor set, see e.g. [8]. ▮

Theorem 3.3. *The completion $\mathbb{Z}^G$ has no nonzero nilpotent elements. Each element $b \in G$ is a non-zero-divisor in $\mathbb{Z}^G$. If G is divisor dense, then $\mathbb{Z}^G$ has characteristic zero.*

Proof.

1. $\mathbb{Z}^G$ has no non-zero nilpotent elements x: Let $x^m = 0$ where $x = [(x_n)]$. Then for all $i \in G$ there is an N_i such that $i^m \mid x_n^m$ for all $n \geq N_i$, since G is a semigroup. Hence $i \mid x_n$ for all $n \geq N_i$ and therefore $x = 0$.

2. Let $b \in G$ and let a be an element of $\hat{\mathbb{Z}}$ such that $b \cdot a = 0$. Let $a = [(a_i)]$ where (a_i) is Cauchy. Then $ba_i \to 0$ so for all $i \in G$ there is an N_i such that $i \mid ba_j$ for all $j \geq N_i$. Applying this to bi implies $i \mid a_j$ and hence $a_j \to 0$ so therefore $a = 0$. Hence b is a non-zero-divisor.

3. $\mathbb{Z}^G$ has characteristic zero: let p be a prime number and let a be an element of $\mathbb{Z}^G$ such that $p \cdot a = 0$. Since G is divisor complete there is a $b \in G$ such that $p \mid b$. Then $b \cdot a = 0$ so $a = 0$. ▮

The following is a concrete realization of the result [4] for zero dimensional compact rings:

Theorem 3.4. *Let G be a semigroup. There exists a family $(I_n : n \in G)$ of ideals in $\mathbb{Z}^G$, that consists of sets that are both open and closed (hence compact), satisfies $a \mid b \implies I_b \subset I_a$ for all $a, b \in G$, and is a basis of neighborhoods of 0 in $\mathbb{Z}^G$.*

Proof. If $b \in G$ let $I_b = \overline{N_{0,b}}$, where the closure is taken in $\mathbb{Z}^G$ and $N_{a,b}$ is the same doubly infinite arithmetic progression in $\mathbb{Z}$ defined above. Since $N_{0,b}$ is an ideal, so is I_b.

Claim: $\mathbb{Z}^G = \cup_{a=1}^b \overline{N_{0,b}}$ where the union is disjoint. To see this note firstly that $\cup_{a=1}^b \overline{N_{0,b}} = \overline{\mathbb{Z}} = \mathbb{Z}^G$. If $x \in \overline{N_{a,b}} \cap \overline{N_{a',b}}$, then there are Cauchy sequences (x_n) and (x'_n) such that $a + x_n b \to x$ and $a' + x'_n b \to x$. But this means that for all $i \in G$, $i \mid a + x_n b - x$ and $i \mid a' + x'_n b - x$ for all $n \ge N_i$ so $i \mid a - a' + (x_n - x'_n)b$. Choosing $i = b$ we get $b \mid a - a'$ so $a = a'$. Therefore the union is disjoint. This implies each I_b is open as well as closed.

We can write $I_b = b\mathbb{Z}^G$ (since if (bx_n) is Cauchy so is (x_n)), and therefore $a \mid b$ implies $I_b \subset I_a$.

Finally note that, for each $b \in G$, $I_b = \{x \in \mathbb{Z}^G : v(x) \le 1/n_j\}$ where n_j is the integer appearing in the definition of v with $n_j = \max\{\mathrm{n_i} : \mathrm{n_i} \mid \mathrm{b}\}$, so the (I_b) are a basis of neighborhoods of 0 and generate the topology on $\mathbb{Z}^G$. ▮

Theorem 3.5. *Let $p \in G$ be a rational prime. Then p is prime in $\mathbb{Z}^G$.*

Proof. Let $p = xy$ where $x = [(x_n)]$ and $x = [(x_n)]$ where (x_n) and (y_n) are Cauchy. Since $p \mid x_n y_n - p$ for all $n \ge N_1$, $p \mid x_n y_n$ so $p \mid x_n$ or $p \mid y_n$, and thus either $p \mid x_n$ or $p \mid y_n$ for an infinite number of integers $n \in \mathbb{N}$.

Suppose $p \mid x_n$ for an infinite number of $n \in \mathbb{N}$. Then, since (x_n) is Cauchy, $p \mid x_n$ for all $n \ge N_2$. Let $pz_n = x_n$ for these n. Then (z_n) is Cauchy, and if we let $z = [(z_n)]$, $p = pzy$ in $\mathbb{Z}^G$. Therefore $ip \mid pz_n y_n - p$ for all $i \in G$ with $i \ge N_3$, so $i \mid z_n y_n - 1$ and hence $1 = zy$ in $\mathbb{Z}^G$. Therefore $x = pz$ where z is a unit, so x is prime in $\mathbb{Z}^G$. ▮

Example 3.2. Let $p \in G$ be a rational prime and $I = \overline{N_{0,p}} = p\hat{\mathbb{Z}}$ be the principal ideal generated by p. It follows of course from the above theorem that I is maximal. However we illustrate these ideas with a direct proof: Let M be an ideal such that $I \subset M$ and $x \in M \setminus I$. Since $x \notin I$, $p \nmid x$ so $x = [(x_n)]$ where (x_n) can be chosen such that $p \nmid x_n$ for all n. For each $n \in \mathbb{N}$, let y_n^1 and y_n^2 be integers satisfying $y_n^1 x_n + p y_n^2 = 1$. Since $\mathbb{Z}^G$ is sequentially compact, there exists a subsequence (n_j) of $\mathbb{N}$ such that $y_{n_j}^1 \to y^1, y_{n_j}^2 \to y^2$, and $x_{n_j} \to x$ in $\hat{\mathbb{Z}}$. If follows that $yx + py = 1$ so $1 \in M$. Hence I is maximal.

4. CLOSED SUBSETS AND MAPPINGS FOR $(\mathbb{Z}, \tau)$

In this section the topology is always the full topology τ.

THEOREM 4.1. *For $k = 1, 2, 3, \cdots$ let $S_k = \{n^k : n \in \mathbb{N} \cup \{0\}\}$. If k is even then S_k is closed. If k is odd then*

$$\overline{S_k} = S_k \cup \{-S_k\}.$$

In both cases the closure of S_k is perfect in $(\mathbb{Z}, \tau)$.

Proof. 1. Let $k = 2l$ be even and suppose $a \in \overline{S_k} \setminus S_k$. Then $N_{a,3a^2} \cap S_k \neq \emptyset$ so there exist integers x, y such that

$$a + 3xa^2 = a(1 + 3xa) = y^k.$$

But $(a, 1 + 3xa) = 1$ so, for some $b \mid y$ with $b \geq 1$, $a = -b^k$. Then $y^{2l} + b^{2l} = 3xa^2$ and

$$(\frac{y}{b})^{2l} + 1 = 3xa.$$

But this is impossible since the left hand side is congruent to either 1 or 2 mod 4 and 3 divides the right hand side.

2. Let $k > 2$ be odd and let $a \geq 1$, $b \geq 1$ be given. Note that there is a $c \in \mathbb{N}$ with $a^k + a^k(b-1)^k = bc$, so if $d = a(b-1)$, $d \geq 0$ and $b \mid a^k + d^k$. Therefore $-a^k + bc = d^k$ so $N_{-a^k,b} \cap S_k \neq \emptyset$. Therefore $-a^k \in \overline{S_k}$.

Conversely, if $a \notin S_k$ and for all $b \geq 1$, $N_{a,b} \cap S_k \neq \emptyset$, then $N_{a,a^2} \cap S_k \neq \emptyset$, so $a + a^2x = y^k$ for integers x, y and therefore $a = -d^k$ for some $d \geq 1$.

3. To show $\overline{S_k}$ is perfect, observe that since $n! \to 0$, $(-n! + a)^k \to a^k$ so every k'th power is a limit of distinct k'th powers. Hence $\overline{S_k}$ has no isolated points.

4. If $k = 1$ then $\mathbb{Z} = \overline{S_1} = S_1 \cup -S_1$. ∎

Note that the result does not of course apply when $k = 1$.

THEOREM 4.2. *The closure of the set of prime integers in $(\mathbb{Z}, \tau)$ is*

$$\overline{\mathbb{P}} = \mathbb{P} \cup \{-1, 1\}.$$

Proof. If $x \in \mathbb{Z} \backslash \{-1, 0, 1\}$ then $N_{x,2|x|} \cap \mathbb{P}$ is $\{x\}$ if $x \in \mathbb{P}$ and $\emptyset$ otherwise, since $x + 2n|x| = x(1 \pm 2n)$. Thus $\mathbb{P}$ includes none of its cluster points and no point in the complement of $\mathbb{P} \cup \{-1, 0, 1\}$ is in $\overline{\mathbb{P}}$. By Dirichlet's theorem, for all $b \geq 1$, $N_{\pm 1,b} \cap \mathbb{P} \neq \emptyset$ so $\pm 1 \in \overline{\mathbb{P}}$. Finally $0 \notin \overline{\mathbb{P}}$ since $N_{0,4} \cap \mathbb{P} = \emptyset$. ∎

Theorem 4.3. *If $k \geq 1$ let $\mathbb{P}_k$ be the set of integers with absolute value having exactly k prime factors (including multiplicity). Let $\mathbb{P}_o = \{-1, 1\}$. Then, for all $k \geq 0$:*
(a) $\mathbb{P}_o \cup \cdots \cup \mathbb{P}_k = \overline{\mathbb{P}_k}$,
(b) $\overline{\mathbb{P}_k} \cup \mathbb{P}_{k+1} = \overline{\mathbb{P}_{k+1}}$,
where the unions in each case are disjoint.

Proof. First two observations. For each $a \in \mathbb{Z}$:
(1) for all $b \geq 1$ there is a $c \in N_{a,b}$ with the number of prime factors $\Omega(c) = \Omega(a) + 1$, namely $c = a + 2nab$, where n has been chosen so that $1 + 2nb$ is prime,
(2) if $\Omega(a) = k$ then all elements c of $N_{a,2|a|}$ have $\Omega(c) \geq k$.

(a) By (1), $\mathbb{P}_k \subset \overline{\mathbb{P}_{k+1}}$ so the left hand side is a subset of the right hand side. By (2), for $j > k$, $\overline{\mathbb{P}_{k+1}} \cap \mathbb{P}_j = \emptyset$. Since

$$\mathbb{Z} = \bigcup_{k=0}^{\infty} \mathbb{P}_k \cup \{0\}$$

it follows that

$$\mathbb{P}_{k+1} \subset \mathbb{P}_o \cup \cdots \cup \mathbb{P}_{k+1} \cup \{0\}.$$

But 0 is not in $\overline{\mathbb{P}_{k+1}}$ since every element c of $N_{0,b} \setminus \{0\}$ has $\Omega(c) \geq \Omega(b)$, and $\Omega(b)$ can be made arbitrarily large. Hence the right hand side is a subset of the left hand side and (a) follows.

(b) This is really just a restatement of (a). ∎

Another way to express (a): the set of integers with less than or equal to k prime factors is closed in $(\mathbb{Z}, \tau)$.

Theorem 4.4. *For all $a, b \in \mathbb{Z}$ the maps $x \to ax + b$ are closed and open for $(\mathbb{Z}, \tau)$.*

Proof. Since the maps $x \to -x$ and $x \to x + b$ are homeomorphisms, we need only show that for $a \geq 1$ the map $x \to ax$ is closed.

Let $F \subset \mathbb{Z}$ be closed and let $x_n \in F$ be such that $ax_n \to \alpha$ in τ. Then for all $i \geq 1$ there is an $N_i \geq 1$ such that for all $n \geq N_i$, $i \mid ax_n - \alpha$. Choose $i = a$ to show $a \mid \alpha$. Let $\alpha = a\beta$ so $i \mid a(x_n - \beta)$. Now choose $i = aj$ to see that $j \mid x_n - \beta$ so $x_n \to \beta$. Hence $\beta \in F$ so the mapping is closed.

For all non-zero a, $aN_{r,s} = N_{ar,|a|s}$ so the maps are open also. ∎

Theorem 4.5. *Let $p \in \mathbb{Z}[x]$ be a polynomial. Then $p : (\mathbb{Z}, d) \to (\mathbb{Z}, d)$ is uniformly continuous.*

Proof. If $n_i \mid x - y$ then $n_i \mid p(x) - p(y)$ so $\langle p(x) - p(y)\rangle \geq x - y$. ▮

The potential domain of application of this result is clear: first show it is true for a multinomial $p : \mathbb{Z}[x_1, \cdots, x_n] \to \mathbb{Z}$. (Note that multinomials are continuous, but not necessarily uniformly continuous.) Use uniform continuity to extend each multinomial to a continuous mapping $\hat{p} : \hat{\mathbb{Z}}[x_1, \cdots, x_n] \to \hat{\mathbb{Z}}$, so the set $F = \hat{p}^{-1}\{0\}$ is a compact subset of $\hat{\mathbb{Z}}^n$. Then use compactness of study properties of F, for example its size.

5. EXAMPLES

If F is a compact subset of $\mathbb{P}$, then F is a finite set. This is because compact subsets are closed and have no cluster points.

Dirichlet's theorem on primes in an arithmetic progression was used in Theorem 4.1 to show that $\overline{\mathbb{P}} = \mathbb{P} \cup \{-1, 1\}$. Conversely, this relationship implies a special case of Dirichlet's theorem, usually proved using cyclotomic polynomials, namely that there exist an infinite number of primes in every arithmetic progression of the form $an+1$ and $an-1$ for every $a \geq 1$. To see this consider the case $an+1$. Since $N_{1,a} \cap \mathbb{P} \neq \emptyset$ there is a prime p_1 and integer n_1 such that $p_1 = an_1 + 1$. The result now follows inductively, first replacing $N_{1,a}$ by $N_{1,a} \setminus \{p_1\}$ etc.

Now let the set of primes be divided into two disjoint subsets, $\mathbb{P} = A \sqcup B$. Let $\langle A\rangle$ represent the symmetric multiplicative semigroup in $\mathbb{Z}$ generated by A, i.e.

$$\langle A\rangle = \{\pm {p_1}^{\alpha_1} \cdots {p_m}^{\alpha_m} : m \in \mathbb{N}, \alpha_i \geq 0, p_i \in A\}.$$

Theorem 5.1. *The interior of $\langle A\rangle$ is empty in $(\mathbb{Z}, \tau)$ if and only if the number of primes in B is infinite.*

Proof. Let $|B| < \infty$ so $F = \cup_{p\in B} N_{0,p}$ is closed in $(\mathbb{Z}, \tau)$. If $P = \mathbb{Z} \setminus F$ then P is open and non-empty, because if $q \notin B$ is prime, then $q \in P$. If $n \in P$

$$n = \pm \prod p_i^{\alpha_i}$$

where no $p_i \in B$. Hence $n \in \langle A\rangle$. Therefore $P \subset \langle A\rangle$ so the interior is not empty.

Now let $\langle A\rangle \neq \emptyset$ so some $N_{a,b} \subset \langle A\rangle$. Then $N_{a,b} = (a, b)(\alpha + \beta\mathbb{Z})$ where $(\alpha, \beta) = 1$. But given $p \in \mathbb{P}$, $p \mid \beta$ implies that for all $n \in \mathbb{Z}$, $p \nmid \alpha + n\beta$, and $p \nmid \beta$ implies there is an $n \in \mathbb{Z}$ such that $p \mid \alpha + n\beta$. Hence the only primes which can be missing from A are among prime divisors of β, which are finite in number. Hence B has a finite number of elements. ▮

We say a subset A of a topological space X is discrete if all points of A are isolated in X. In the theorem below, the metric d is the same as that defined in Theorem 3.1 above.

THEOREM 5.2. *Let A be a non-empty subset of $\mathbb{Z}$ with $0, \pm 1 \notin A$ and $(a,b) = 1$ if $a, b \in A$ with $a \neq b$. If A is complete in $(\mathbb{Z}, d)$, then A is finite.*

Proof. For each $a \in A$, $N_{a,2|a|} \cap A = \{a\}$, so the derived set $A' = \emptyset$ and A is discrete. Embed A in the completion $\hat{\mathbb{Z}}$ using the standard embedding a goes to the class of the constant sequence with value a. Then A is closed hence compact in the completion, hence squentially compact in the completion, therefore in $\mathbb{Z}$, so it is compact in $\mathbb{Z}$. Since A is discrete and compact it must be finite. ▮

EXAMPLE 5.1. For $n = 0, 1, \cdots$ let $f_n = 2^{2^n} + 1$ so $\mathbb{F} = \{f_n\}$ is the Fermat numbers. Then $\mathbb{F}$ is closed and discrete in $(\mathbb{Z}, \tau)$: Let $f_{n_i} \to \alpha \neq 0$ with $n_1 < n_2 < \cdots$. Since $|\alpha| \mid f_{n_i} - \alpha$ for n_i sufficiently large, $\alpha \mid f_{n_i}$. Therefore $\alpha \mid (f_{n_i}, f_{n_{i+1}}) = 1$ so $\alpha = \pm 1$. But $1 \notin \overline{\mathbb{F}}$ since $3 \mid 2^{2^{n_j}}$ is false.

Also $0 \notin \overline{\mathbb{F}}$ since $N_{0,2} \cap \mathbb{F} = \emptyset$, and finally,$-1 \notin \overline{\mathbb{F}}$ since $4 \nmid 2^{2^{n_i}} + 1 - (-1)$. Hence $\mathbb{F}$ is closed in $(\mathbb{Z}, \tau)$. It is discrete since $(f_n, f_m) = 1$ for $n \neq m$.

EXAMPLE 5.2. Let $\mathbb{M} = \{m_p = 2^p - 1 : p \in \mathbb{P}\}$ be the Mersenne numbers. Then $\mathbb{M}$ is closed and discrete in $(\mathbb{Z}, \tau)$.

We assume the following well known property of divisors of the Mersenne number m_p: If $n \mid m_p$ then $n \equiv \pm 1 \mod 8$ and $n \equiv 1 \mod p$, see for example [7].

Firstly $0 \notin \overline{\mathbb{M}}$ since $m_p \in N_{0,2} \cap \mathbb{M}$ implies $2 \mid m_p$ but $2 \not\equiv \pm 1(\mod 8)$.

If $\alpha \neq 0$ is such that $m_{p_i} \to \alpha$ then $\alpha \mid m_{p_i}$ so $\alpha \equiv 1 \mod p_i$. But we can choose $p_1 < p_2 < \cdots$ and in particular such that $|\alpha| < p_i$, so necessarily $\alpha = 1$. If then $m_p \in N_{1,4} \cap \mathbb{M}$, there is an integer n such that $2^p - 1 = 1 + 4n$ which is impossible for $p \geq 2$. Hence $\mathbb{M}$ is closed.

Let $p_1 < p_2 < \cdots < p_n$ be all the primes up to p_n and suppose m_{p_n} is a cluster point of $\mathbb{M}$. Then

$$\mathbb{M} \cap N_{m_{p_n}, 2^{p+1}} \setminus \{2^{p_1} - 1, \cdots, 2^{p_n} - 1\} \neq \emptyset.$$

Therefore there is a prime $q > p_n$ with $2^p - 1 + n2^{p+1} = 2^q - 1$ so $2^q = 2^p(2n+1)$ which is impossible. Therefore $\mathbb{M}$ is discrete.

EXAMPLE 5.3. Let $Sf = \{\pm n : n \geq 2 \text{ squarefree}\}$. Then Sf is perfect in $(\mathbb{Z}, \tau)$: Sf is closed since if the squarefree sequence $n_i \to \alpha$ then $\alpha \mid n_i$

so α is squarefree. Every point of Sf is a cluster point because if a is squarefree and $b \geq 1$ then $N_{a,b} \setminus \{a\}$ contains a square free element: write $a + nb = (a, b)(\alpha + n\beta)$ where $(\alpha, \beta) = 1$. Since the arithmetic progression $\alpha + n\beta$ has an infinite number of prime values, chose one which does not divide (a, b) so that the corresponding $a+nb$ will be square free and distinct from a.

Example 5.4. Let $U = \{u_n : n = 0, 1, 2, \cdots\}$ be the Fibonacci numbers where $u_0 = 0, u_1 = 1$ and $u_{n+2} = u_{n+1} + u_n$ for all $n \geq 0$. Then

1. The point 0 is a cluster point of U, i.e. $0 \in U'$. This is because for all $b \geq 1$, there is an n such that $b \mid u_n$.

2. Every point congruent to 4 mod 8 is not in $\overline{U}$: If for some n and l, $u_n = 4 + 8l$, then $4 \mid u_n$ so $6 \mid n$ which implies $8 = u_6 \mid u_n$, so $8 \mid 4$ which is impossible. This can be written $U \cap N_{4,8} = \emptyset$.

3. Similarly it may be shown that $U \cap N_{6,12} = \emptyset$ and also that $U \cap N_{7,21} = \emptyset$.

4. More generally, it follows from Proposition 5.1 following this summary , that if $(i, j) = 1$ or 2 then there is a $b \geq 1$ such that $a = u_i u_j$ implies $U \cap N_{a,b} = \emptyset$.

5. Summary: It follows from 2,3 and 4 above that the following points of $\mathbb{Z} \setminus U$ are not in $\overline{U}$: $\{-6, -4, 4, 6, 7, 10, 12\}$.

6. Finally we show the point -1 is in the closure of U: To see this use the identity $u_{m+n} + (-1)^n u_{m-n} = u_m v_n$, where (v_n) are the Lucas numbers. Let $b \geq 1$ be given. As in 1. above chose m such that $b \mid u_m$. If m is even let $n = m - 1$, and if m is odd let $n = m - 2$. Then in both cases n is odd and $m - n = 1$ or $m - n = 2$, so $b \mid u_m v_n = u_{m+n} - 1$. In other words $U \cap N_{-1,b} \neq \emptyset$ so $-1 \in \overline{U}$.

7. **Conjecture**: The closure of U in $(\mathbb{Z}, \tau)$ is $U \cup V$ where $V = \{(-1)^{n+1} u_n : n \in \mathbb{N}\}$.

Some numerical evidence for the truth of this conjecture comes from consideration of the intersection of the compliment of the basic open sets $N_{a,b}$ with the following given values of a and b, all being such that their intersection with U is empty:

$a \in \{4, 6\},\ b = 8,$
$a \in \{4, 6, 7, 9\},\ b = 11,$
$a \in \{6\},\ b = 12,$
$a \in \{4, 6, 7, 9\},\ b = 13,$
$a \in \{4, 6, 10, 12, 14\},\ b = 16,$
$a \in \{6, 7, 10, 11\},\ b = 17,$
$a \in \{4, 6, 7, 9, 11, 12, 14\},\ b = 18,$
$a \in \{4, 6, 7, 9, 10, 12, 14\},\ b = 19,$
$a \in \{4, 6, 7, 9, 10, 11, 12, 14, 15, 16, 17, 19\},\ b = 21,$
$a \in \{4, 7, 16, 19\},\ b = 23,$
$a \in \{4, 6, 9, 11, 12, 14, 15, 18, 19, 20, 22\},\ b = 24,$
$a \in \{4, 6, 7, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 27\},\ b = 29$

To check these, simply consider the values of the Fibonacci numbers modulo b for one complete period. The intersection of their compliments exactly identifies $\{U \cup V\} \cap [-1000, 1000]$.

The following proposition is used in item 4. above.

Proposition 5.1. *(a) Let $(i, j) = 1$, $i, j \geq 3$. Then*

$$u_n = u_i u_j + u_i u_j u_{ij} l$$

has no solution in integers $n \geq 3$ and $l \in \mathbb{Z}$.
(a) If $(i, j) = 2$, $i, j \geq 3$. Then

$$u_n = u_i u_j + u_i u_j u_{ij/2} l$$

has no solution.

Proof. (a) Let $n \geq 3$, $i, j \geq 3$, $(i, j) = 1$, and $l \in \mathbb{Z}$ be such that

$$u_n = u_i u_j + u_i u_j u_{ij} l \tag{1}$$

Then $u_i \mid u_n$ and $u_j \mid u_n$ and therefore $i \mid n$ and $j \mid n$ and therefore $ij \mid n$ so $u_{ij} \mid u_n$. Equation (1) then implies $u_{ij} \mid u_i u_j$. But $(u_i, u_j) = u_{(i,j)} = u_1 = 1$, so $u_{ij} = u_i u_j$.

If $\alpha = \frac{1+\sqrt{5}}{2}$ then we can write $u_n = [\frac{\alpha^n}{\sqrt{5}} + \frac{1}{2}]$ therefore

$$\frac{\alpha^{ij}}{\sqrt{5}} - \frac{1}{2} \leq (\frac{\alpha^i}{\sqrt{5}} + \frac{1}{2})(\frac{\alpha^j}{\sqrt{5}} + \frac{1}{2})$$

so

$$\alpha^{ij} \leq \frac{a^{i+j}}{\sqrt{5}} + \frac{\alpha^i + \alpha^j}{2} + \frac{3\sqrt{5}}{4}. \tag{2}$$

But $1 < \alpha$ and therefore $\alpha^{ij} \leq c\alpha^{i+j}$ where $c = \frac{1}{\sqrt{5}} + \frac{1}{2} + \frac{3\sqrt{5}}{4}$. Therefore

$$ij \leq \frac{\log c}{\log \alpha} + i + j.$$

where $2 < i, j$. This equation has no solutions, hence neither does (1).

(b) Let $n \geq 3$, $l \in \mathbb{Z}$ and $i, j \geq 4$ be such that $(i, j) = 2$. Let

$$u_n = u_i u_j + u_i u_j u_{ij/2} l. \tag{3}$$

Using a similar argument to that given in (a) it follows that

$$u_{ij/2} = u_i u_j. \tag{4}$$

Let $i = 2r$ and $j = 2s$ so $u_{2r} u_{2s} = u_{2rs}$. Therefore

$$\frac{\alpha^{2rs}}{\sqrt{5}} - \frac{1}{2} \leq (\frac{\alpha^{2r}}{\sqrt{5}} + \frac{1}{2})(\frac{\alpha^{2s}}{\sqrt{5}} + \frac{1}{2}).$$

Using the same argument as that given in (a), but replacing α by α^2, we obtain the inequality

$$rs \leq \frac{\log c}{2 \log \alpha} + r + s$$

where $r, s \geq 2$, so $rs < 2 + r + s$. The only solution to this inequality is $(r, s) = (2, 3)$ or $(3, 2)$. In that case

$$u_i u_j = u_4 u_6 = 24 \neq 144 = u_{12}$$

so equation (4) is never true. Therefore (3) has no solutions. ∎

ACKNOWLEDGMENT

The support of the Department of Mathematics at the University of Waikato, and discussions with Ian Hawthorn and Tom Körner are warmly acknowledged, as are suggestions made by John Cremona, especially those relating to the use of the inverse limit to describe the completion.

REFERENCES

1. Apostol, T.M. *Introduction to Analytic Number Theory*. New York, Berlin, Heidelberg: Springer-Verlag, 1976.
2. Aigner, M. and Ziegler, G. M, *Proofs from the Book*, Springer-Verlag, 1998.
3. Engelking, R. *Outline of General Topology*, North-Holland, 1968.
4. Kaplansky, I. *Topological Rings*, Amer. J. Math. **69** (1947), 153-183.
5. Mahler, K. *P-adic numbers and their functions.*, Cambridge, Cambridge University Press, 1981
6. Morris, S. A. *Pontryagin Duality and the structure of locally compact abelian groups* London Mathematical Society Lecture Notes in Mathematics **29**, Cambridge, 1977.
7. Ribenboim, P. *The New Book of Prime Number Records*, Springer-Verlag, 1999.
8. Schoenfeld, A. H. and Gruenhage, G. *An alternate characterization of the Cantor set*, Proc. Amer. Math. Soc. **53**, (1975), 235-236.
9. Sierpinski, W. *Sur une propriété topologique des ensembles dénombrables denses en soi*, Fundam. Math. **1**, (1920), 11-16.