Definition 1. For any set of positive naturals A, let $S(A) = \{\text{prime } p : \exists a \in A \text{ s.t. } p|a\}$ be its **prime shadow**

Consider the following statements:

i A is infinite and $S(A)$ is finite

ii $\exists a, b \in S$ such that $a|b$ and $a \neq b$.

iii There exist infinitely many pairs $a, b \in A$ with $a \neq b$ such that $a|b$.

iv $\exists a_1, a_2, \ldots \in A$ with $a_1|a_2|a_3|\cdots$

v There exists a finite subset B of A such that $\forall a \in A \setminus B \exists a_1, a_2, \ldots \in A$ with $a|a_1|a_2|a_3|\cdots$

We will succesively prove that i implies ii, iii, iv, and finally v.

Lemma 2. i $\implies$ ii

Proof. Since $S(A)$ is finite, we can express $S(A)$ as $\{p_1, p_2, \ldots, p_n\}$. Every element in A can be expressed as $p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$ for some nonnegative integers $e_1, \ldots, e_n$. Let $f : A \to \mathbb{N}^n$ take an element a to the n-tuple $(e_1, e_2, \ldots, e_n)$ such that $a = p_1^{e_1}\cdots p_n^{e_n}$. Then for $1 \leq i \leq n$ let $f_i(a)$ be the i-coordinate of $f(a)$.

We will prove i $\Longrightarrow$ ii by induction on the size of $S(A)$. As a base case, if $|S(A)| = 1$ then every element of A is a power of p_1. In that case, for any pair (a, b), either $a|b$ or $b|a$.

Now assume that for any infinite set B with prime shadow of size $n-1$ there exists a pair $b_1, b_2 \in B$ such that $b_1|b_2$. Suppose to the contrary that there does not exists a pair (a, b) such that $a|b$. Then for all pairs (a, b) there must exist an i such that $f_i(a) > f_i(b)$. Now fix $x \in A$. For all $a \in A$ there is an i with $f_i(a) < f_i(x)$. By the pigeonhole principle, there must be some j such that for infinitely many $a \in A$, $f_j(a) < f_j(x)$. Again by the pigeonhole principle we know that for some $e < f_j(x)$ there are infinitely many $a \in A$ such that $f_j(a) = e$.

Let

$$B = \left\{ \prod_{i \neq j} p_i^{f_i(a)} : a \in A \text{ s.t. } f_j(a) = e \right\}$$

We have $S(B) = S(A)\setminus\{p_j\}$, and B is infinite, therefore there exists a pair $b_1, b_2 \in B$ such that $b_1|b_2$. Then $b_1p_j^e$ and $b_2p_j^e$ are elements of A and $b_1p_j^e|b_2p_j^e$. Thus we have completed the induction. $\square$

As a side note, the above proof can be used to show that only finitely many numbers a in A are not part of a pair $a, b \in A$ such that either $a|b$ or $b|a$. But this is stronger than we need.

Lemma 3. i $\implies$ iii

Proof. We will prove that for any natural k there exist $a_1, \ldots, a_k \in A$ with $a_1|a_2|\cdots|a_k$ by inducting on k. Lemma 2 gives us the base case with $k = 2$. So, assume that the statement is true for $k-1$. If we consider the set

$$D = \left\{ \mathbf{a} = (a_1, \ldots, a_{k-1}) \in A^{k-1} : a_1|a_2|\cdots|a_{k-1} \right\}$$

If this where finite, then we can take the set

$$A' = \{a \in A : \neg\exists \mathbf{d} \in D, 0 \leq i \leq k-1 \text{ s.t. } d_i = a\}$$

This is still an infinite set if D is finite. But then our inductive hypothesis gives us a tuple $(d_1, d_2, \ldots, d_{k-1}) \in D^{k-1}$ with $d_1|\cdots|d_{k-1}$, contradicting the definition of D. Therefore D must be infinite.

Now, consider the set

$$B = \{a \in A : \exists \mathbf{d} \in D \text{ s.t. } d_{k-1} = a\}$$

We want to show that B is infinite, so suppose to the contrary that B is finite. Then B has a maximum element b_m. But then $D \subseteq \{1, \ldots, b_m\}^{k-1}$, which would mean that D is finite, even though we proved it was infinite. Therefore, B must be infinite.

Then lemma 2 guarantees us a pair $b_1, b_2 \in B$ such that $b_1|b_2$. Then there are some $a_1, \ldots, a_{k-1}$ such that $a_1|\cdots|a_{k-2}|a_{k-1} = b_1$. Then we have the k-tuple $(a_1, \ldots, a_{k-2}, b_1, b_2)$ with $a_1|\cdots|a_{k-2}|b_1|b_2$, so we have completed the induction.

That means that there must be an infinite chain of divisibility in A because we showed that there is no maximum length for a chain of divisibility. □

Theorem 4. If A is an infinite subset of $\mathbb{N}_+$ that has a finite prime shadow, then for cofinitely many $a \in A$, there exist $a_1, a_2, a_3, \ldots$ all in A with $a_1 = a$ such that for all $i > 0$, $a_i|a_{i+1}$. Informally, if A is an infinite subset of $\mathbb{N}_+$ with finite prime shadow, then cofinitely many elements of A are part of an infinite ascending chain of divisibility.

Proof. Let B be the set of elements that are not are not part of an infinite chain of divisibility.

$$B = \left\{a : \neg\exists(a_1, a_2, \ldots) \in A^{\mathbb{N}} \text{ s.t. } a|a_1|a_2|\cdots\right\}$$

Suppose B is infinite. Then lemma 3 tells us that there exists an infinite chain of divisibility in B. But that contradicts the definition of B, so B must be finite. □

Corollary 5. There are infinitely many primes

Proof. Start with $a_1 = 2$. Then iteratively define a_i as

$$1 + \prod_{n=1}^{i-1} a_i$$

Then for all i, j, a_i and a_j are relatively prime. Then let $A = \{a_i : i \in \mathbb{N}\}$. This is an infinite set that has no infinite chain of divisibility, therefore $S(A)$ cannot be finite. Thus there must be infinitely many primes. □