$\mathbb{ITYM}$ 2021 - Problem 2:
Sequences of Coprime Integers.

Team France

Composed by :

De Ridder Achille, Harter Louis-Max,
Fourcin Emile, Quille Maxime
Varnet Philémon, Leroux Hubert

Supervised by :

Lenoir Théo et Béreau Antoine

June 2021

June 2021

Contents

Introduction

Notations

We use the following notations :

- $\mathbb{P}$ the set of prime numbers ;
- (a, b) the PGCD of $a, b \in \mathbb{Z}$, when the context is clear ;
- the CRT for Chinese Reminder Theorem
- $\mathcal{P}(E) := \{p \in \mathbb{P} \mid \exists a \in E, p \mid a\}$ the set of the prime divisors of a set E.
- we define, for an increasing sequence (a_i) of positive integers, $\mathbf{DP}(a_i) := \mathcal{P}(a_i - a_j \mid i > j)$

Lemma 1. *Let $(a_i)_{i \in I}$ be a finite or infinite increasing sequence of positive integers. Then $\mathbf{DP}(a_i)$ is finite if and only if $(a_i)_{i \in I}$ is.*

Proof. If $(a_i)_{i \in I}$ is finite, then it is clear that $\mathbf{DP}(a_i)$ is. Now if $(a_i)_{i \in I}$ is infinite ($I = \mathbb{N}$), suppose for the sake of contradiction $\mathbf{DP}(a_i)$ finite. Then, for fixed $\ell_1 \neq \ell_2 \in \mathbb{N}$, $\mathcal{P}(a_i - a_{\ell_1} \mid i > \ell_1), \mathcal{P}(a_i - a_{\ell_2} \mid i > \ell_2) \subseteq \mathbf{DP}(a_i)$ are also finite, but this contradicts Kobayashi's theorem over sets of prime divisors. ∎

Questions

0.1 For $k = 2$

0.1.1 n-prime sequences for infinitely many $n \in \mathbb{N}$

Proposition 1. *Let $a_1 < a_2$ be a sequence of two positive integers. There are infinitely many $n \in \mathbb{N}$ for which the sequence is n-prime.*

Proof. Let there be positive integers $a_1 < a_2$. It is enough to consider the $n = \ell(a_2 - a_1) - a_1 + 1$ for $n = \ell \in \mathbb{N}$ large enough, so that $n \geqslant 1$. Indeed, we have then

$$(a_1 + n, a_2 + n) = (a_2 - a_1, a_1 + n) = (a_2 - a_1, \ell(a_2 - a_1) + 1) = 1$$

The set of such ℓ being infinite, it is the same for the n one (to which, for each of them, corresponds a unique ℓ), as desired. ∎

0.1.2 n-prime sequences for all $n \in \mathbb{N}$

Proposition 2. *Let $a_1 < a_2$ be a sequence of two positive integers. Such sequence is n-prime for all $n \in \mathbb{N}$ if and only if $a_2 = a_1 + 1$.*

Proof. Suppose that $a_2 > a_1 + 1$, that is $a_2 - a_1 > 1$. Then there exists $p \in \mathbb{P}$ such that $p \mid a_2 - a_1$. There exists infinitely many $n \in \mathbb{N}$ such that $n \equiv -a_1 \pmod{p}$, so that $p \mid (a_2 - a_1, n + a_1) = (a_2 + n, a_1 + n)$. So $a_1 < a_2$ can't be n-prime for all $n \in \mathbb{N}$. Reciprocally, if $a_2 = a_1 + 1$, then for all $n \in \mathbb{N}$,

$$(a_2 + n, a_1 + n) = (a_2 - a_1, a_1 + n) = (1, a_1 + n) = 1$$

∎

0.2 For $k = 3$

0.2.1 n-prime sequences for infinitely many $n \in \mathbb{N}$

Proposition 3. *Let $a_1 < a_2 < a_3$ be a sequence of three positive integers. There are infinitely many $n \in \mathbb{N}$ for which the sequence is n-prime.*

Proof. Let $a_1 < a_2 < a_3$ be a sequence of three positive integers. Let $d = (a_2 - a_1, a_3 - a_1)$. We can see that

$$d = (a_2 - a_1, a_3 - a_1) = (a_2 - a_1, a_3 - a_2) = (a_3 - a_1, a_3 - a_2)$$

It is then enough to consider the $n \in \mathbb{N}$ such that

$$\begin{cases} n \equiv 1 - a_1 \pmod{a_2 - a_1} \\ n \equiv 1 - a_1 \pmod{a_3 - a_1} \\ n \equiv 1 - a_2 \pmod{a_3 - a_2} \end{cases}$$

which admits an infinite number of solutions in $\mathbb{N}$ according to the CRT, since this system is consistent : $a_2 \equiv a_1 \pmod{d}$ hence $1 - a_1 \equiv 1 - a_2 \pmod{d}$. We then have

$$\begin{aligned} (a_1 + n, a_2 + n) &= (k(a_2 - a_1) + 1, a_2 - a_1) = 1 \\ (a_1 + n, a_3 + n) &= (\ell(a_3 - a_1) + 1, a_3 - a_1) = 1 \\ (a_2 + n, a_3 + n) &= (m(a_3 - a_2) + 1, a_3 - a_2) = 1 \end{aligned}$$

as desired. ∎

0.2.2 n-prime sequences for all $n \in \mathbb{N}$

Proposition 4. *There are no sequence of positive integers $a_1 < a_2 < a_3$ n-prime for all $n \in \mathbb{N}$.*

Proof. Suppose for the sake of contradiction that the sequence of positive integers $a_1 < a_2 < a_3$ is n-prime for all $n \in \mathbb{N}$. By Proposition 2, since $a_1 < a_2$ and $a_1 < a_3$ must be n-prime for all $n \in \mathbb{N}$ too, we have $a_3 = a_1 + 1$ and $a_2 = a_1 + 1$, so $a_3 = a_2$ which is a contradiction. ∎

0.3 For $k \geqslant 4$

0.3.1 n-prime sequences for all $n \in \mathbb{N}$

Proposition 5. *For $k \geqslant 4$, there are no sequence of positive integers $(a_i)_{1 \leqslant i \leqslant k}$ n-prime for all $n \in \mathbb{N}$.*

Proof. It's a direct corollary of Proposition 4, since if $(a_i)_{1 \leqslant i \leqslant k}$ were n-prime for all $n \in \mathbb{N}$, it would be also the case for the sequence $a_1 < a_2 < a_3$. ∎

0.3.2 non n-prime sequences for all $n \in \mathbb{N}$

Proposition 6. *For $k \geqslant 4$, there exists sequences of positive integers $(a_i)_{1 \leqslant i \leqslant k}$ which aren't n-prime for all $n \in \mathbb{N}$.*

Proof. Let's consider a sequence of positive integers $b_1 < b_2 < b_3 < b_4$ which isn't n-prime for all $n \in \mathbb{N}$, for example the sequence of general term $b_i = i$ for all $1 \leqslant i \leqslant 4$. Indeed, if $m \in \mathbb{N}$ is even, then $(b_2 + m, b_4 + m) = (m + 2, m + 4) = (m + 2, 2) = (m, 2) = 2$, so it isn't m-prime

; if m is odd, $(b_1 + m, b_3 + m) = (m + 1, m + 3) = (m + 1, 2) = (m - 1, 2) = 2$ so it isn't m-prime.
It is then sufficient to consider a sequence of positive integers $a_1 < \ldots < a_k$ such that $a_i = b_i$ for all $1 \leqslant i \leqslant 4$ for such a sequence $(b_i)_{1 \leqslant i \leqslant 4}$. Indeed, if it were n-prime for some $n \in \mathbb{N}$, the sequence $(b_i)_{i \leqslant i \leqslant 4}$ would be too, an absurdity. ■

0.4 General case for finite sequences

0.4.1 n-prime sequences for all $n \in \mathbb{N}$

Proposition 7. *According to Proposition 2, Proposition 4 and Proposition 5, a positive and increasing sequence of integers $(a_i)_{1 \leqslant i \leqslant k}$ for $k \geqslant 2$ is n-prime for all $n \in \mathbb{N}$ if and only if $k = 2$ and $a_2 = a_1 + 1$.*

0.4.2 non n-prime sequences for all $n \in \mathbb{N}$

Definition 1 (invasive sequence)**.** It is said that a sequence $(a_i)_{1 \leqslant i \leqslant k}$ with values in $\mathbb{N}$ is *invasive* if there exists $p \in \mathbf{DP}(a_i)$ such that each element of $\mathbb{Z}_p$ has at least 2 antecedents by (the canonical projection of) $(a_i)_{1 \leqslant i \leqslant k}$.

Proposition 8. *A increasing sequence of positive integers $(a_i)_{1 \leqslant i \leqslant k}$ isn't n-prime for all $n \in \mathbb{N}$ if and only if it's invasive.*

Proof. Let $(a_i)_{1 \leqslant i \leqslant k}$ be a increasing sequence with values in $\mathbb{N}$.

• Suppose $(a_i)_{1 \leqslant i \leqslant k}$ is invasive. Let $n \in \mathbb{N}$. Then there exists $i > j$ in $[\![1, k]\!]$ and $p \in \mathbb{P}$ such that $a_i \equiv a_j \equiv -n \pmod{p}$, hence $p \mid a_i + n$ and $p \mid a_i + n$ so $p \mid (a_i + n, a_j + n)$ which implies that $(a_i)_{1 \leqslant i \leqslant k}$ is not n-prime.

• Conversely, if it is not invasive, then, by setting $p_1, \ldots, p_\ell$ the elements of $\mathbf{DP}(a_i)$, for all $i \in [\![1, \ell]\!]$, there exists $r_i \in \mathbb{Z}_{p_i}$ having at most 1 antecedent by $(a_i)_{1 \leqslant i \leqslant k}$. Let's then take $m \in \mathbb{N}$ solution of

$$\begin{cases} x \equiv -r_1 \pmod{p_1} \\ x \equiv -r_2 \pmod{p_2} \\ \qquad\vdots \\ x \equiv -r_\ell \pmod{p_\ell} \end{cases}$$

which exists by the CRT. Now let $i > j$ in $[\![1, k]\!]$; we can see that for any prime divisor p of $a_i - a_j$, $p = p_s$ for some $s \in [\![1, \ell]\!]$, so that $m + a_t \equiv 0 \pmod{p_s} \Leftrightarrow a_t \equiv r_s \pmod{p_s}$ is true for at most one $t \in \{i, j\}$, hence p cannot simultaneously divide $a_i + m$, $a_j + m$, so it does not divide $(a_i + m, a_j + m) = (a_i - a_j, a_j + m)$. Since $\mathcal{P}\left((a_i - a_j, a_j + m)\right) \subseteq \mathbf{DP}(a_i)$, this gcd must be 1. $(a_i)_{1 \leqslant i \leqslant k}$ is therefore m-prime and is therefore not m-prime for all $n \in \mathbb{N}$. ■

0.4.3 n-prime sequences for infinitely many $n \in \mathbb{N}$

Lemma 2. *Let be an integer $k \geqslant 2$ and $(a_i)_{i \leqslant k}$ increasing finite sequence of positive integers m-prime for some $m \in \mathbb{N}$. Then it is n-prime for infinitely many $n \in \mathbb{N}$.*

Proof. Let be an integer $k \geqslant 2$ and $(a_i)_{1 \leqslant i \leqslant k}$ such a sequence, m-prime for some $m \in \mathbb{N}$. We will construct an integer $m' > m$ (and even infinitely many) such that $(a_i)_{1 \leqslant i \leqslant k}$ is m'-prime which will be enough to conclude. Let $m' = m + r \cdot \operatorname{lcm}_{i>j}(a_i - a_j)$ where $r \in \mathbb{N}$, which are clearly infinite. Then for all $\ell > \ell' \in [\![1, k]\!]$:

$$(a_\ell + m', a_{\ell'} + m') = \left(a_\ell - a_{\ell'}, a_{\ell'} + m + r \cdot \operatorname{lcm}_{i>j}(a_i - a_j)\right) = (a_\ell - a_{\ell'}, a_{\ell'} + m) = (a_\ell + m, a_{\ell'} + m) = 1$$

which concludes the lemma. ■

This result warrant that a increasing sequence of positive integers is n-prime for infinitely many $n \in \mathbb{N}$ if it is for some $m \in \mathbb{N}$, the reciprocal of the lemma being obvious. From the previous point (Proposition 8), we obtain the following proposition :

Proposition 9. *a finite sequence is n-prime for infinitely many $n \in \mathbb{N}$ if it isn't invasive.*

In particular, for $k = 2$, for any prime divisor p of $a_2 - a_1$, we cannot have $\bar{a_1}, \bar{a_2} = \mathbb{Z}_p$ and $\bar{a_2} = \bar{a_1}$ so the sequence is n-prime for infinitely many $n \in \mathbb{N}$, as seen in Proposition 1. When $k = 3$, for any prime divisor p of $(a_2 - a_1)(a_3 - a_1)(a_3 - a_2)$, we cannot have $\{\bar{a_1}, \bar{a_2}, \bar{a_3}\} = \mathbb{Z}_p$ and $\bar{a_1} = \bar{a_i}$ for $i \in \{2, 3\}$ and, for $\ell \in \{2, 3\} \setminus \{i\}$, $\bar{a_\ell} = \bar{a_j}$ for $j \in \{1, i\}$ which implies $\bar{a_1} = \bar{a_2} = \bar{a_3}$. We then find the result in Proposition 2.

0.5 General case for infinite sequences

0.5.1 sequences n-prime for all $n \in \mathbb{N}$

Proposition 10. *There isn't any infinite, increasing sequence of positive integers that is n-prime for all $n \in \mathbb{N}$.*

Proof. Let $(a_i)_{i \in \mathbb{N}}$ be a increasing sequence of positive integers,n n-prime for all $n \in \mathbb{N}$. Then any finite sub-sequence of length greater than 4 of $(a_i)_{i \in \mathbb{N}}$ is n-prime for all $n \in \mathbb{N}$, which is absurd according to Proposition 5. Therefore there is no infinite n-prime sequence for all $n \in \mathbb{N}$ ■

0.5.2 n-prime sequences for infinitely many $n \in \mathbb{N}$

We have a partial answer to this question, by showing that there are infinitely many infinite sequences that are n-prime for infinitely many n.

Definition 2 (A-prime sequence)**.** A finite or infinite sequence of increasing integers is said to be *A-prime* for a subset A of $\mathbb{N}$ when it is n-prime for all $n \in A$.

Definition 3 (A-covering sequence)**.** We say that a sequence $(a_i)_{1 \leqslant i \leqslant k}$ is *A-covering* if there exists $p \in \mathbb{P}$ such that for any $j \in \mathbb{N}$, there exists $n \in A$ such that $p \mid n + a_j$. It is thus said to be *not A-covering* if, for any $p \in \mathbb{P}$, there exists $j \in \mathbb{N}$ such that for any $n \in A$, $p \nmid a_j + n$.

Lemma 3 (1 bis)**.** *Let $(a_i)_{1 \leqslant i \leqslant k}$ be a increasing sequence of integers with $k \geqslant 2$, A-prime for some finite $A \subseteq \mathbb{N}$ and not A-covering. Then there exists $h \in \mathbb{N} \setminus A$ such that $(a_i)_{1 \leqslant i \leqslant k}$ is $A \cup \{h\}$-prime and not $A \cup \{h\}$-covering.*

Proof. we take any element n of A, and set $M := a_k + \max A$ then $h := n + M!$. In the same way as in Lemma 2, since for all $i > j \in [\![1, k]\!]$, $a_i - a_j < a_i + 1 \leqslant M$ hence $\operatorname{lcm}_{i>j}(a_i - a_j) \mid M!$ so $(a_i)_{1 \leqslant i \leqslant k}$ is $A \cup \{h\}$-prime.
For its not $A \cup \{h\}$-covering character, let's take $p \in \mathbb{P}$.

- If $p \leqslant M$, then $p \mid M!$ and by hypothesis there exists $j \in [\![1,k]\!]$ such that for any $s \in A$, $p \nmid a_j + s$. In particular $p \nmid a_j + n$ so $p \nmid a_j + n + M! = a_j + h$, and so $p \nmid a_j + s$ for all $s \in A \cup \{h\}$.

- If $p > M$, then, since $k \geqslant 2$ and $a_1 < a_2 < \ldots < a_k < M < p$, by the pigeonhole principle there exists $j \in [\![1,k]\!]$ such that $a_j + h \not\equiv 0 \pmod p$ i.e. $p \nmid a_j + h$. Now, for all $s \in A$, $a_j + s \leqslant M < p$ so $p \nmid a_j + s$ for all $s \in A \cup \{h\}$.

Therefore, there exists $j \in [\![1,k]\!]$ such that $p \mid a_j + n$ for any $n \in A \cup \{h\}$ for any prime p, i.e. $(a_i)_{1 \leqslant i \leqslant k}$ is not $A \cup \{h\}$-covering. ■

Lemma 4. *Let $(a_i)_{1 \leqslant i \leqslant k}$ be a increasing sequence of integers, A-prime for some finite $A \subseteq \mathbb{N}$ and not A-covering. Then there exists an integer $a_{k+1} > a_k$ such that $(a_i)_{1 \leqslant i \leqslant k+1}$ is A-prime and not A-covering.*

Proof. Let us pose again $M := a_k + \max A$. Let $p_1, \ldots, p_\ell$ be the prime numbers less than M where $\ell \geqslant 1$. For any $j \in [\![1,\ell]\!]$, there exists $i_j \in [\![1,k]\!]$ such that $p \nmid a_{i_j} + s$ for any $s \in A$. Let's take $a_{k+1} > a_k$ solution of the system :

$$\begin{cases} x \equiv a_{i_1} \pmod{p_1} \\ x \equiv a_{i_2} \pmod{p_2} \\ \qquad \vdots \\ x \equiv a_{i_\ell} \pmod{p_\ell} \end{cases}$$

that exists by the CRT. Then for all $i \in [\![1,k]\!]$ and $n \in A$, any prime divisor p of $a_i + n$ verifies $p \leqslant a_i + n \leqslant M$ so $p = p_j$ for some $j \in [\![1,\ell]\!]$ hence $a_{k+1} + n \equiv a_{i_j} + n \not\equiv 0 \pmod{p_j}$ i.e. $p \nmid a_{k+1} + n$. By A-primality of $(a_i)_{1 \leqslant i \leqslant k}$, we know that, for all $n \in A$, for all $i \neq j \in [\![1,k]\!]$, $(a_i + n, a_j + n) = 1$. Now for any $i \in [\![1,k]\!]$, if a prime p divides $a_i + n$, it doesn't divide $a_{k+1} + n$ so $(a_i + n, a_{k+1} + n) = 1$. Thus, $(a_i)_{1 \leqslant i \leqslant k+1}$ is A-prime. It's as well clearly A-covering, since we can take the same $j \in [\![1,k]\!]$ as for the non A-covering character of $(a_i)_{1 \leqslant i \leqslant k}$. ■

Lemma 5. *There exist infinitely many triples $(a_1, a_2, n) \in \mathbb{N}^3$ with $a_1 < a_2$ such that $(a_i)_{i=1,2}$ is n-prime and non $\{n\}$-covering.*

Proof. In the case $k = 2$, $\{n\}$-covering is equivalent to $\{n\}$-primality. Lemma 2 gives us that for any given positive integers $a_1 < a_2$, there exists an infinite number of n such that $(a_i)_{i=1,2}$ is n-prime, hence $\{n\}$-prime and $\{n\}$-covering. ■

Proof of Proposition 10. We recursively construct the sequences $(a_n)_{n \in \mathbb{N}}$ and $(A_n)_{n \in \mathbb{N}}$ such that, for all $n \in \mathbb{N}$, $(a_i)_{1 \leqslant i \leqslant n}$ is strictly increasing, A_n-prime and non A_n-covering, and $|A_n| = n$.

- By **Lemma 4**, we take any $(a_1, a_2, m) \in \mathbb{N}^3$ such that $(a_i)_{i=1,2}$ is increasing, A_1-prime and non A_1-covering with $A_1 := \{m\}$.

- For all $n \geqslant 1$, with **Lemma 2** and **Lemma 3**, we can find $a_{n+1} > a_n$ and $A_{n+1} = A_n \cup \{h_n\}$ where $h_n \in \mathbb{N}$ such that $(a_i)_{1 \leqslant i \leqslant n+1}$ is increasing, A_{n+1}-prime and non A_{n+1}-covering. We also have $|A_{n+1}| = n + 1$.

We can now take $(a_n)_{n \in \mathbb{N}}$, increasing and A-prime for $A := \bigcup_{n \in \mathbb{N}} A_n$. ■

0.5.3 non n-prime sequence for all $n \in \mathbb{N}$

We did not find a necessary and sufficient condition on such sequences that makes the problem "really simpler", we think that the question is too large to have a short answer.

Of course, if there an infinite sequence of positive integers contains a finite sub-sequence that is non n-prime for all n, it's the case for the infinite sequence. Unfortunately, this is not a necessary condition.

Proposition 11. *There exist infinitely many increasing sequence of positive integers $(a_i)_{i\in\mathbb{N}}$ non n-prime for all $n \in \mathbb{N}$ such that any finite subsequence $(b_i)_{i\in I}$ (with finite $I \subseteq \mathbb{N}$) of $(a_i)_{i\in\mathbb{N}}$ is n-prime for some $n \in \mathbb{N}$.*

Proof. Let $a \in \mathbb{N}$. We show that the sequence $(a_i)_{i\in\mathbb{N}} = (p_i + a)_{i\in\mathbb{N}}$ fits, where $(p_i)_{i\in\mathbb{N}}$ is the enumeration of $\mathbb{P}$ in increasing order.

- it's a non n-prime sequence for all $n \in \mathbb{N}$: let $n \in \mathbb{N}$. Because $a+n > 0$, there exists $j \in \mathbb{N}$ s.t. $p_j \nmid a+n$, so $(p_j, a+n+p_j) = 1$. By Dirichlet's Theorem on arithmetic progressions, there exists $i \neq j$ s.t $p_i \equiv p_j \pmod{a+n+p_j}$. So $(a_i - a_j, a+n+p_j) = a+n+p_j > 1$ for j sufficiently big.
- let $(b_i)_{i\in I}$ a finite sub-sequence of (a_i). Then, by taking $n \equiv -a \pmod{\prod_{i>j}(b_i - b_j)}$ sufficiently big, we have, for all $u > v \in \mathbb{N}$: $(b_u + n, b_v + n) = (b_u - b_v, p_v + a + n) = (b_u - b_v, p_v) = (p_u - p_v, p_v) = (p_u, p_v) = 1$ so $(b_i)_{i\in I}$ is n-prime.

■

$P(n)$-prime sequences

It is assumed that P is arbitrary and fixed beforehand in all that follows.

0.6 the finite case

Definition 4 (P-invasive sequence)**.** It is said that a sequence $(a_i)_{1\leqslant i\leqslant k}$ with values in $\mathbb{N}$ is *P-invasive* if there exists $p \in \mathbf{DP}(a_i)$ such that each element of $P(\mathbb{Z}_p)$ has at least 2 antecedents by (the canonical projection of) $(a_i)_{1\leqslant i\leqslant k}$.

Proposition 12. *A increasing sequence of positive integers $(a_i)_{1\leqslant i\leqslant k}$ isn't n-prime for all $n \in \mathbb{N}$ if and only if it's P-invasive.*

Proof. This is essentially an adaptation of the case of Proposition 8 (where $P = X$) which does not bring any difficulty. ■

Lemma 6. *If a finite and infinite sequence of positive integers is $P(n)$-prime for a certain $n \in \mathbb{N}$, then it is n'-prime for a certain $n \in \mathbb{N}$.*

Proof. Let $(a_i)_{i\leqslant k}$ a such sequence with $k \geqslant 2$. Then by Proposition 12, for all $p_i \in \{p_1, \ldots, p_N\} := \mathbf{DP}(a_i)$, there exists $n_i \in P(\mathbb{Z}_{p_i})$ such that $P(n_i)$ has at most 1 antecedent by (a_i). Let $n' \in \mathbb{N}$ a solution of the system :

$$\begin{cases} x \equiv P(n_1) \pmod{p_1} \\ x \equiv P(n_2) \pmod{p_2} \\ \qquad\vdots \\ x \equiv P(n_N) \pmod{p_N} \end{cases}$$

which exists by CRT again. If there exists $i \neq j \leqslant k$ such that $(a_i+n', a_j+n') = (a_i-a_j, a_i+n') > 1$, then there exists p_ℓ where $\ell < N$ s.t. $a_i \equiv a_j \pmod{p_\ell}$ and $a_i \equiv -n' \equiv -P(n_\ell) \pmod{p_\ell}$, so $p_\ell \mid (a_i - a_j, a_i + P(n_\ell))$, a contradiction. So $(a_i)_{i\leqslant k}$ is n'-prime. ■

0.6.1 $P(n)$-prime sequence for infinitely many $n \in \mathbb{N}$

Lemma 7. *Let be an integer $k \geqslant 2$ and $(a_i)_{i\leqslant k}$ increasing finite sequence of positive integers $P(m)$-prime for some $m \in \mathbb{N}$. Then it is $P(n)$-prime for infinitely many $n \in \mathbb{N}$.*

Proof. We use the same arguments as in Lemma 2, by noting that if $m \equiv m' \pmod{p}$, then $P(m) \equiv P(m') \pmod{p}$. ■

The case $P = X^k$ for a certain $k \geqslant 1$

Let $p \in \mathbb{P}$. A known result is that $\mathbb{Z}_p \to \mathbb{Z}_p : x \mapsto x^k$ is bijective (*i.e.* surjective since $\mathbb{Z}_p$ is finite) if and only if $(p-1, k) = 1$. This leads to the following :

Proposition 13. *If $P(X) = X^k$ and for all $p \in \mathbf{DP}(a_i)$, $(p-1, k) = 1$, then $(a_i)_{i\leqslant k}$ is n^k-prime for a certain $n \in \mathbb{N}$ if and only if it is n'-prime for a certain $n' \in \mathbb{N}$.*

General Case for P

Definition 5 (Permutation Polynomial)**.** Let p a prime number. We say that a polynomial with integers coefficients is a *Permutation Polynomial* (**PP**) of $\mathbb{Z}_p$ if $x \mapsto P(x)$ is a bijection of $\mathbb{Z}_p$.

Last proposition leads us to the following :

Proposition 14. *Let $(a_i)_{i\leqslant k}$ a finite increasing sequence of positive integers. If P is a* **PP** *of $\mathbb{Z}_p$ for all $p \in \mathbf{DP}(a_i)$, is $P(n)$-prime for a certain $n \in \mathbb{N}$ if and only if it is n'-prime for a certain $n' \in \mathbb{N}$.*

Proof. A sense is directly given by Lemma 6. The other one is true by using CRT on antecedents of n by $\mathbb{Z}_p \to \mathbb{Z}_p : x \mapsto P(x)$, that exists since P is a **PP** of $\mathbb{Z}_p$, for all $p \in \mathbf{DP}(a_i)$. ■

Proposition 15 (Hermite's Criterion)**.** *A polynomial with integers coefficients P is a* **PP** *of $\mathbb{Z}_p$ for a certain $p \in \mathbb{P}$ if and only if :*

- *P has exactly one root in $\mathbb{Z}_p$*
- *For each $t \in \mathbb{N}$ such that $t \leqslant q-2$ and $p \nmid t$, the reduction of $P(X)^t \mod X^p - X$ has degree $\leqslant p-2$.*

A proof of this statement is given by Theorem 1.6 in *Permutation Polynomials of Finite Fields* by Christopher J. Shallue.
This could be useful to check if a polynomial P is a **PP** of $\mathbb{Z}_p$ for all $p \in \mathbf{DP}(a_i)$ for special P, when $(a_i)_{i\in I}$ is finite. But what can we say if it's infinite? Lemma 1 avoid us to use this technique.