$\mathbb{ITYM}$ 2021 - Problem 2: Sequences of coprime integers

Presented by Philémon Varnet
France

Definition : n-prime sequence

For a sequence of integers $a_1, a_2, \dots$ (finite or infinite), we say it is *n-prime* for some $n \in \mathbb{N}$ if all the terms

$$a_1 + n, a_2 + n, a_3 + n, \dots$$

are pairwise coprime.

Notations

- (a, b) the GCD of $a, b \in \mathbb{Z}$
- $\mathcal{P}(E) := \{p \in \mathbb{P} \mid \exists a \in E, p \mid a\}$ the set of the prime divisors of a set E.
- we define, for an increasing sequence (a_i) of positive integers, $\mathbf{DP}(a_i) := \mathcal{P}(a_i - a_j \mid i > j)$

Notations

- (a, b) the GCD of $a, b \in \mathbb{Z}$
- $\mathcal{P}(E) := \{p \in \mathbb{P} \mid \exists a \in E, p \mid a\}$ the set of the prime divisors of a set E.
- we define, for an increasing sequence (a_i) of positive integers, $\mathbf{DP}(a_i) := \mathcal{P}(a_i - a_j \mid i > j)$

Notations

- (a, b) the GCD of $a, b \in \mathbb{Z}$
- $\mathcal{P}(E) := \{p \in \mathbb{P} \mid \exists a \in E, p \mid a\}$ the set of the prime divisors of a set E.
- we define, for an increasing sequence (a_i) of positive integers, $\mathbf{DP}(a_i) := \mathcal{P}(a_i - a_j \mid i > j)$

General case for finite sequences

Proposition 7 : a positive and increasing sequence of integers $(a_i)_{1 \leqslant i \leqslant k}$ for $k \geqslant 2$ is n-prime for all $n \in \mathbb{N}$ iff $k = 2$ and $a_2 = a_1 + 1$.

General case for finite sequences

Invasivity : It is said that a sequence $(a_i)_{1\leqslant i\leqslant k}$ of positive integers 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 $(a_i)_{1\leqslant i\leqslant k}$.

Examples :

The sequence $(a_i)_{i\leqslant 4} = (2, 5, 6, 9)$ gives $\mathbf{DP}(a_i) = \{2, 3, 7\}$ so it is invasive with $p = 2$ (2 odd and 2 even numbers).

The sequence $(1, 2, 3)$ gives $\mathbf{DP}(a_i) = \{2\}$ so it is not invasive (only 1 even).

General case for finite sequences

Invasivity : It is said that a sequence $(a_i)_{1\leqslant i\leqslant k}$ of positive integers 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 $(a_i)_{1\leqslant i\leqslant k}$.

Examples :

The sequence $(a_i)_{i\leqslant 4} = (2, 5, 6, 9)$ gives $\mathbf{DP}(a_i) = \{2, 3, 7\}$ so it is invasive with $p = 2$ (2 odd and 2 even numbers).

The sequence $(1, 2, 3)$ gives $\mathbf{DP}(a_i) = \{2\}$ so it is not invasive (only 1 even).

General case for finite sequences

Invasivity : It is said that a sequence $(a_i)_{1\leqslant i\leqslant k}$ of positive integers 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 $(a_i)_{1\leqslant i\leqslant k}$.

Examples :
The sequence $(a_i)_{i\leqslant 4} = (2,5,6,9)$ gives $\mathbf{DP}(a_i) = \{2,3,7\}$ so it is invasive with $p = 2$ (2 odd and 2 even numbers).

The sequence $(1,2,3)$ gives $\mathbf{DP}(a_i) = \{2\}$ so it is not invasive (only 1 even).

General case for finite sequences

- **Proposition 8** : A finite increasing sequence of positive integers $(a_i)_{1\leqslant i\leqslant k}$ isn't n-prime for all $n \in \mathbb{N}$ iff it's invasive.
- **Proposition 9** : A finite increasing sequence of positive integers is n-prime for infinitely many $n \in \mathbb{N}$ iff it isn't invasive.

General case for infinite sequences

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

Sketch of proof : such infinite sequence would contain a subsequence of arbitrary length n-prime for all n, contradicting prop. 5.

General case for infinite sequences

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

Sketch of proof : such infinite sequence would contain a subsequence of arbitrary length n-prime for all n, contradicting prop. 5.

General case for infinite sequences

Now we look at sequences which are n-prime for infinitely many $n \in \mathbb{N}$.

We define :

- A-**primality** : 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 $n \in A$.

- A-**coveringness** : 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 $n \in A$, $p \nmid a_j + n$.

General case for infinite sequences

Now we look at sequences which are n-prime for infinitely many $n \in \mathbb{N}$.

We define :

- A-**primality** : 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 $n \in A$.

- A-**coveringness** : 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 $n \in A$, $p \nmid a_j + n$.

General case for infinite sequences

Now we look at sequences which are n-prime for infinitely many $n \in \mathbb{N}$.

We define :

- A-**primality** : 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 $n \in A$.
- A-**coveringness** : 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 $n \in A$, $p \nmid a_j + n$.

General case for infinite sequences

Proposition 11 : There exist infinitely many infinite, increasing sequences of positive integers that are n-prime for infinitely many $n \in \mathbb{N}$.

Sketch of proof : we use the following algorithm to generate $(a_i)_{i\in\mathbb{N}}$ and A (an infinite set) s.t. (a_i) is A-prime:

General case for infinite sequences

Proposition 11 : There exist infinitely many infinite, increasing sequences of positive integers that are n-prime for infinitely many $n \in \mathbb{N}$.

Sketch of proof : we use the following algorithm to generate $(a_i)_{i \in \mathbb{N}}$ and A (an infinite set) s.t. (a_i) is A-prime:

General case for infinite sequences

Algorithm 1 Generate $(a_i)_{i\in\mathbb{N}}$ and A

Generate (a_1, a_2, n) s.t. $a_1 < a_2$ is n-prime and not $\{n\}$-covering (exists by Lemma 5)
$A_1 \leftarrow \{n\}$
$k \leftarrow 2$
loop
  Generate a_{k+1} s.t. $(a_i)_{i\leqslant k+1}$ is A_k-prime (exists by Lemma 3)
  Generate A_{k+1} s.t. $(a_i)_{i\leqslant k+1}$ is A_{k+1}-prime, not A_{k+1}-covering and $|A_{k+1}| = k+1$ (exists by Lemma 4)
  $k \leftarrow k+1$
end loop
$A \leftarrow \bigcup_{k\in\mathbb{N}} A_k$

General case for infinite sequences

Partial answer : any infinite sequence containing a finite not n-prime for all n sequence is not n-prime for all n too. However, it is not a necessary criteria :

Proposition 12 : 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 $n \in \mathbb{N}$.

Sketch of proof : we prove that all the sequences of the form $(p_i + a)_{i \in \mathbb{N}}$ where $a \in \mathbb{N}$ fit.

General case for infinite sequences

Partial answer : any infinite sequence containing a finite not n-prime for all n sequence is not n-prime for all n too. However, it is not a necessary criteria :

Proposition 12 : 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 $n \in \mathbb{N}$.

Sketch of proof : we prove that all the sequences of the form $(p_i + a)_{i\in\mathbb{N}}$ where $a \in \mathbb{N}$ fit.

General case for infinite sequences

Partial answer : any infinite sequence containing a finite not n-prime for all n sequence is not n-prime for all n too. However, it is not a necessary criteria :

Proposition 12 : 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 $n \in \mathbb{N}$.

Sketch of proof : we prove that all the sequences of the form $(p_i + a)_{i \in \mathbb{N}}$ where $a \in \mathbb{N}$ fit.

finite $P(n)$-prime sequences

Most of the previous results does not generalize with $P(n)$-prime sequences.

For example, if $P(X) = X^2 - X$ and a sequence of even integers, then it is not $P(n)$-prime for all n.

In the other way, for example if for all $p \in \mathbf{DP}(a_i)$ and all $i \in [\![1, k]\!]$, $a_i \not\equiv 0 \pmod p$ and $P(X) = \prod_{p \in \mathbf{DP}(a_i)} (X^p - X)$, then the sequence is n-prime for all n.

finite $P(n)$-prime sequences

Most of the previous results does not generalize with $P(n)$-prime sequences.

For example, if $P(X) = X^2 - X$ and a sequence of even integers, then it is not $P(n)$-prime for all n.

In the other way, for example if for all $p \in \mathbf{DP}(a_i)$ and all $i \in [\![1, k]\!]$, $a_i \not\equiv 0 \pmod{p}$ and $P(X) = \prod_{p \in \mathbf{DP}(a_i)} (X^p - X)$, then the sequence is n-prime for all n.

finite $P(n)$-prime sequences

Most of the previous results does not generalize with $P(n)$-prime sequences.

For example, if $P(X) = X^2 - X$ and a sequence of even integers, then it is not $P(n)$-prime for all n.

In the other way, for example if for all $p \in \mathbf{DP}(a_i)$ and all $i \in [\![1, k]\!]$, $a_i \not\equiv 0 \pmod p$ and $P(X) = \prod_{p \in \mathbf{DP}(a_i)} (X^p - X)$, then the sequence is n-prime for all n.

finite $P(n)$-prime sequences

But some results generalize!

P-**invasivity** : We say that a sequence $(a_i)_{1\leqslant i\leqslant k}$ 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 $(a_i)_{1\leqslant i\leqslant k}$.

Proposition 13 : An increasing sequence of positive integers $(a_i)_{1\leqslant i\leqslant k}$ isn't n-prime for all $n \in \mathbb{N}$ iff it's P-invasive.

finite $P(n)$-prime sequences

But some results generalize!

P-**invasivity** : We say that a sequence $(a_i)_{1\leqslant i\leqslant k}$ 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 $(a_i)_{1\leqslant i\leqslant k}$.

Proposition 13 : An increasing sequence of positive integers $(a_i)_{1\leqslant i\leqslant k}$ isn't n-prime for all $n \in \mathbb{N}$ iff it's P-invasive.

finite $P(n)$-prime sequences

But some results generalize!

P-**invasivity** : We say that a sequence $(a_i)_{1\leqslant i\leqslant k}$ 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 $(a_i)_{1\leqslant i\leqslant k}$.

Proposition 13 : An increasing sequence of positive integers $(a_i)_{1\leqslant i\leqslant k}$ isn't n-prime for all $n \in \mathbb{N}$ iff it's P-invasive.

finite $P(n)$-prime sequences

We are now interested in the case where $P = X^k$ for some integer $k \geqslant 1$.

For some prime number p, a kwown arithmetical result is that $\mathbb{Z}_p \to \mathbb{Z}_p : x \mapsto x^k$ is bijective iff $(p-1, k) = 1$. This leads to the following :

Proposition 14 : 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 some $n \in \mathbb{N}$ iff it is r-prime for some $r \in \mathbb{N}$.

finite $P(n)$-prime sequences

We are now interested in the case where $P = X^k$ for some integer $k \geqslant 1$.

For some prime number p, a kwown arithmetical result is that $\mathbb{Z}_p \to \mathbb{Z}_p : x \mapsto x^k$ is bijective iff $(p-1, k) = 1$. This leads to the following :

Proposition 14 : 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 some $n \in \mathbb{N}$ iff it is r-prime for some $r \in \mathbb{N}$.

finite $P(n)$-prime sequences

We are now interested in the case where $P = X^k$ for some integer $k \geqslant 1$.

For some prime number p, a kwown arithmetical result is that $\mathbb{Z}_p \to \mathbb{Z}_p : x \mapsto x^k$ is bijective iff $(p-1, k) = 1$. This leads to the following :

Proposition 14 : 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 some $n \in \mathbb{N}$ iff it is r-prime for some $r \in \mathbb{N}$.

finite $P(n)$-prime sequences

Let's remark we just use the fact that
$\mathbb{Z}_p \to \mathbb{Z}_p : x \mapsto P(x)$ is bijective for all $p \in \mathbf{DP}(a_i)$.

We then define :

PP : 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 $\mathbb{Z}_p$.

finite $P(n)$-prime sequences

Let's remark we just use the fact that $\mathbb{Z}_p \to \mathbb{Z}_p : x \mapsto P(x)$ is bijective for all $p \in \mathbf{DP}(a_i)$.

We then define :

PP : 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 $\mathbb{Z}_p$.

finite $P(n)$-prime sequences

Let's remark we just use the fact that $\mathbb{Z}_p \to \mathbb{Z}_p : x \mapsto P(x)$ is bijective for all $p \in \mathbf{DP}(a_i)$.

We then define :

PP : 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 $\mathbb{Z}_p$.

finite $P(n)$-prime sequences

Proposition 15 : 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 $n \in \mathbb{N}$ iff it is r-prime for some $r \in \mathbb{N}$.

Proposition 16 (Hermite's Criterion) : A polynomial with integers coefficients P is a **PP** of $\mathbb{Z}_p$ for some $p \in \mathbb{P}$ iff :

- 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 $\leqslant p-2$.

finite $P(n)$-prime sequences

Proposition 15 : 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 $n \in \mathbb{N}$ iff it is r-prime for some $r \in \mathbb{N}$.

Proposition 16 (Hermite's Criterion) : A polynomial with integers coefficients P is a **PP** of $\mathbb{Z}_p$ for some $p \in \mathbb{P}$ iff :

- 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 $\leqslant p - 2$.

Thank for listening!

For $k = 2$

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.

Sketch of proof : n of the form $\ell(a_2 - a_1) - a_1 + 1$ work.

Example : with $a_1 = 3$, $a_2 = 12$, we take n of the form $9\ell - 2$. Indeed,

$$1 = (10, 19) = (19, 28) = (28, 37) = (37, 46) = \dots$$

For $k = 2$

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.

Sketch of proof : n of the form $\ell(a_2 - a_1) - a_1 + 1$ work.

Example : with $a_1 = 3$, $a_2 = 12$, we take n of the form $9\ell - 2$. Indeed,

$$1 = (10, 19) = (19, 28) = (28, 37) = (37, 46) = \dots$$

For $k = 2$

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.

Sketch of proof : n of the form $\ell(a_2 - a_1) - a_1 + 1$ work.

Example : with $a_1 = 3, a_2 = 12$, we take n of the form $9\ell - 2$. Indeed,

$$1 = (10, 19) = (19, 28) = (28, 37) = (37, 46) = \dots$$

For $k = 2$

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

Sketch of proof : If $a_2 > a_1 + 1$, if p is a prime divisor of $a_2 - a_1$, $n \equiv -a_1 \pmod{p}$ contradicts n-primality. Otherwise $a_1 + n$ and $a_2 + n$ are consecutive so coprime.

For $k = 2$

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

Sketch of proof : If $a_2 > a_1 + 1$, if p is a prime divisor of $a_2 - a_1$, $n \equiv -a_1 \pmod{p}$ contradicts n-primality. Otherwise $a_1 + n$ and $a_2 + n$ are consecutive so coprime.

For $k = 3$

- **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.

  Sketch of proof : We choose appropriate n via CRT.

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

  Sketch of proof : if it is n-prime for all n, it would be the same for its 3 subsequences which yields to a contradiction by prop. 2.

For $k \geqslant 4$

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

  Sketch of proof : direct corollary of prop. 4.

- **Proposition 6** : For $k \geqslant 4$, there exists sequences of positive integers $(a_i)_{1 \leqslant i \leqslant k}$ which arert n-prime for all $n \in \mathbb{N}$.

  Sketch of proof : the sequence defined by $a_k = k$ works by parity.

For $k \geqslant 4$

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

  Sketch of proof : direct corollary of prop. 4.

- **Proposition 6** : For $k \geqslant 4$, there exists sequences of positive integers $(a_i)_{1 \leqslant i \leqslant k}$ which arert n-prime for all $n \in \mathbb{N}$.

  Sketch of proof : the sequence defined by $a_k = k$ works by parity.

For $k \geqslant 4$

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

  Sketch of proof : direct corollary of prop. 4.

- **Proposition 6** : For $k \geqslant 4$, there exists sequences of positive integers $(a_i)_{1 \leqslant i \leqslant k}$ which arert n-prime for all $n \in \mathbb{N}$.

  Sketch of proof : the sequence defined by $a_k = k$ works by parity.

For $k \geqslant 4$

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

  Sketch of proof : direct corollary of prop. 4.

- **Proposition 6** : For $k \geqslant 4$, there exists sequences of positive integers $(a_i)_{1 \leqslant i \leqslant k}$ which arert n-prime for all $n \in \mathbb{N}$.

  Sketch of proof : the sequence defined by $a_k = k$ works by parity.

the sequence of odd squares is non n-prime for all n

Dirichlet's theorem on arithmetic progression : Let m, n coprime positive integers. Then there exist infinitely primes p s.t. $p \equiv m \pmod{n}$.

Law of quadratic reciprocity : Let p, q distinct odd primes. We define the *Legendre symbol* as :

$$\left(\frac{a}{q}\right) = \begin{cases} 1 & \text{if } n^2 \equiv q \mod p \text{ for some integer } n \\ -1 & \text{otherwise} \end{cases}$$

Then :

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$$

the sequence of odd squares is non n-prime for all n

Claim : The sequence of odd squares is non n-prime for all $n \in \mathbb{N}$.

Proof : Let $n \in \mathbb{N}$, and a prime $p \equiv 1 \pmod{8n}$ (which exist since 1 and $8n$ are coprime). We set $n = a^2 m$ where $m = \prod q_i$ is squarefree. Then, by Law of quadratic reciprocity and properties of Legendre symbol :

$$\left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a^2}{p}\right)\left(\frac{2}{p}\right)^{\varepsilon}\prod\left(\frac{q_i}{p}\right)$$

$$= (-1)^{\frac{p-1}{2}} 1^{\varepsilon} \prod \left(\frac{p}{q_i}\right)(-1)^{\frac{(p-1)(q_i-1)}{4}} = 1$$

the sequence of odd squares is non n-prime for all n

So there exist $a \in \mathbb{N}$ such that $a^2 \equiv -n \pmod{p}$. We can suppose a odd since if a is even, $a + p$ is odd. So a^2 is odd, hence a^2 is in the sequence of odd squares, and $(a + 2p)^2$ too, but $a^2 + n \equiv (a + 2p)^2 + n \equiv 0 \pmod{p}$, so $p \mid (a^2 + n, (a + 2p)^2 + n)$ which is then not 1, so the sequence is not n-prime ! $\blacksquare$

finite $P(n)$-prime sequences

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

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

finite $P(n)$-prime sequences

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

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