ON A SYSTEM OF EQUATIONS WITH PRIMES

PAOLO LEONETTI AND SALVATORE TRINGALI

ABSTRACT. Given an integer $n \geq 3$, let $u_1, \ldots, u_n$ be pairwise coprime integers ≥ 2, $\mathcal{D}$ a family of nonempty proper subsets of $\{1, \ldots, n\}$ with "enough" elements, and ε a function $\mathcal{D} \to \{\pm 1\}$. Does there exist at least one prime q such that q divides $\prod_{i \in I} u_i - \varepsilon(I)$ for some $I \in \mathcal{D}$, but it does not divide $u_1 \cdots u_n$?

We answer this question in the positive when the u_i are prime powers and ε and $\mathcal{D}$ are subjected to certain restrictions. We use the result to prove that, if $\varepsilon_0 \in \{\pm 1\}$ and A is a set of three or more primes that contains all prime divisors of any number of the form $\prod_{p \in B} p - \varepsilon_0$ for which B is a finite nonempty proper subset of A, then A contains all the primes.

1. Introduction

Let $\mathbb{P} := \{2, 3, \ldots\}$ be the set of all (positive rational) primes. There are several proofs of the fact that $\mathbb{P}$ is infinite: Some are elementary, others come as a byproduct of deeper results. E.g., six of them, including Euclid's classical proof, are given by M. Aigner and G. M. Ziegler in the first chapter of their lovely *Proofs from THE BOOK* [1]. Although not really focused on the infinity of primes, this paper is inspired by Euclid's original work on the subject, concerned as it is with the factorization of numbers of the form $a_1 \cdots a_n \pm 1$, where $a_1, \ldots, a_n$ are coprime positive integers, and in fact prime powers (we do not consider 1 as a prime power). To be more precise, we first need to fix some notation.

We write $\mathbb{Z}$ for the integers, $\mathbb{N}$ for the nonnegative integers, and $\mathbb{N}^+$ for $\mathbb{N} \setminus \{0\}$, each of these sets being endowed with its usual addition $+$, multiplication $\cdot$ and total order $\leq$ (as is customary, $\geq$ will stand for the dual order of $\leq$).

For a set A, we denote by $|A|$ the cardinality of A, and by $\mathcal{P}_\star(A)$ the family of all finite nonempty *proper* subsets of A, in such a way that $A \notin \mathcal{P}_\star(A)$. Furthermore, for an integer $n \geq 1$ we set $S_n := \{1, \ldots, n\}$ and let $\mathcal{P}_n(A)$ be the collection of all subsets B of A with $|B| = n$.

For the notation and terminology used herein without definition, as well as for material concerning classical topics in number theory, the reader should refer to [7].

With that said, we can state the basic question addressed by the paper:

Question 1. Given an integer $n \geq 3$, pick exponents $v_1, \ldots, v_n \in \mathbb{N}^+$ and (pairwise) distinct primes $p_1, \ldots, p_n \in \mathbb{P}$, and let $\mathcal{D}$ be a nonempty subfamily of $\mathcal{P}_\star(S_n)$ with "enough" elements and ε a map $\mathcal{P}_\star(S_n) \to \{\pm 1\}$. Does there exist at least one prime $q \in \mathbb{P} \setminus \{p_1, \ldots, p_n\}$ such that q divides $\prod_{i \in I} p_i^{v_i} - \varepsilon(I)$ for some $I \in \mathcal{D}$?

2010 *Mathematics Subject Classification.* Primary: 11A05, 11A41, 11A51, 11D61. Secondary: 11D79, 11R27.

Key words and phrases. Agoh-Giuga conjecture, cyclic congruences, Pillai's equation, prime factorization, Znam's problem.

At present, we have no formal definition of what should be meant by the word "enough" in the previous statement: this is part of the question.

With the notation from above it is rather clear, for instance, that the answer to Question 1 is no, at least in general, if $|\mathcal{D}|$ is "small" with respect to n, as shown by the following:

Example 1. Given an integer $k \geq 3$, distinct primes $q_1, \ldots, q_k$ and positive integers $e_1, \ldots, e_k$, let q be the greatest prime dividing at least one of the numbers of the form $\prod_{i \in I} q_i^{e_i} \pm 1$ for $I \in \mathcal{P}_\star(S_k)$.

Then, we get a negative answer to Question 1 by extending $q_1, \ldots, q_k$ to a sequence $q_1, \ldots, q_\ell$ containing all the primes $\leq q$ (note that $\ell \geq k+1$), by taking a nonempty $\mathcal{E} \subseteq \mathcal{P}_\star(S_k)$ and arbitrary $e_{k+1}, \ldots, e_\ell \in \mathbb{N}^+$, and by setting $n := \ell$, $p_i := q_i$, $v_i := e_i$ and $\mathcal{D} := \mathcal{E}$.

Thus, to rule out such trivial cases, one shall suppose, e.g., that $|\mathcal{D}| \geq n\kappa$ or, in alternative, $|\mathcal{D}| \geq n^\kappa$ for some absolute constant $\kappa > 0$.

Specifically, we concentrate here on the case where $\mathcal{D}$ contains at least all subsets of S_n of size 1, $n-2$, or $n-1$, and the restriction of ε to these subsets is constant (see Theorem 1.1 below), while collecting a series of intermediate results that could be useful, in future research, to try to draw broader conclusions.

We observe, in this sense, that Question 1 can be "generalized" as follows:

Question 2. For an integer $n \geq 3$, let $u_1, \ldots, u_n$ be pairwise coprime integers ≥ 2, $\mathcal{D}$ a nonempty subcollection of $\mathcal{P}_\star(S_n)$ for which $\mathcal{D}$ has "enough" elements, and ε a function $\mathcal{P}_\star(S_n) \to \{\pm 1\}$. Does there exist at least one prime q such that q divides $\prod_{i \in I} u_i - \varepsilon(I)$ for some $I \in \mathcal{D}$ and $q \nmid u_1 \cdots u_n$?

Note that Question 2 is not *really* a generalization of Question 1, as the former can be stated in terms of the latter by replacing, with the same notation as above, n with the total number d of the prime divisors of $u_1 \cdots u_n$ and $\mathcal{D}$ with a suitable subfamily of $\mathcal{P}_\star(S_d)$.

Questions 1 and 2 are somewhat reminiscent of cyclic systems of simultaneous congruences, studied by several authors, and still in recent years, for their connection with some long-standing questions in the theory of numbers, and especially Znám's problem and the Agoh-Giuga conjecture (see [5] and [8], respectively, and references therein).

Our initial motivation has been, however, of a completely different sort, and in fact related to the following:

Problem 1. Let A be a subset of $\mathbb{P}$, having at least three elements, and such that for any $B \in \mathcal{P}_\star(A)$ all prime divisors of $\prod_{p \in B} p - 1$ belong to A. Then $A = \mathbb{P}$.

This served as a problem in the 4th grade of the 2003 Romanian IMO Team Selection Test, and it appears (up to minor notational differences) as Problem 10 in [2, p. 53]. The solution provided in the book (p. 62) consists of two parts. In the first one, the authors aim to show that A is infinite, but their argument is seen to be at least incomplete. Specifically, their argument is as follows (we use the notation from above):

After having proved that 2 is in A, they suppose by contradiction that A is a finite set of size k (where $k \geq 3$) and let $p_1, \ldots, p_k$ be a numbering of A such that $2 = p_1 < \cdots < p_k$.

Then, they derive from the standing assumptions on A that

$$p_2^\alpha + 1 = 2^{\beta+1} p_2^\gamma + 2$$

for some $\alpha, \beta, \gamma \in \mathbb{N}$. But this does not imply $1 \equiv 2 \bmod p_2$ (as is stated in the book) unless $\gamma \neq 0$, which is nowhere proved and has no obvious reason to be true.

The problem *per se* is not, however, difficult, and it was used also for the 2004 France IMO Team Selection Test (we are not aware of any official solution published by the organizers of the competition).

Questions somewhat similar to those above have been considered by other authors, even though under different assumptions, and mostly focused on the properties of the prime factorization of particular sequences (of integers) $a_0, a_1, \ldots$ recursively defined, e.g., by formulas of the form $a_{n+1} = 1 + a_0 \cdots a_n$; see [12, §1.1.2] and the references therein for an account (for all practical purposes, we notice here that one of the questions raised by A. A. Mullin in [11] and mentioned by W. Narkiewicz on page 2 of his book has been recently answered in [3]).

Now, we have not been able to work out a complete solution of Question 1, whatever this may be. Instead, as already remarked, we solve it in some special cases. This is in fact the content of the following theorem, which is also the main result of the paper:

Theorem 1.1. *Given an integer $n \geq 3$, pick distinct primes $p_1, \ldots, p_n$, exponents $v_1, \ldots, v_n \in \mathbb{N}^+$ and a subcollection $\mathcal{D}$ of $\mathcal{P}_\star(S_n)$ such that $\mathcal{D}_0 \subseteq \mathcal{D}$, where*

$$\mathcal{D}_0 := \mathcal{P}_1(S_n) \cup \mathcal{P}_{n-2}(S_n) \cup \mathcal{P}_{n-1}(S_n).$$

Then, for every function $\varepsilon : \mathcal{P}_\star(S_n) \to \{\pm 1\}$ such that the restriction of ε to $\mathcal{D}_0$ is constant, there exists at least one $q \in \mathbb{P} \setminus \{p_1, \ldots, p_n\}$ such that q divides $\prod_{i \in I} p_i^{v_i} - \varepsilon(I)$ for some $I \in \mathcal{D}$.

The proof of Theorem 1.1, as presented in Section 3, requires a number of preliminary lemmas, which are stated and proved under assumptions much weaker than those in the above statement.

In particular, we will make use at some point of the following result [13]:

Theorem 1.2 (Zsigmondy's theorem)**.** *Pick $a, b \in \mathbb{N}^+$ and an integer $n \geq 2$ such that (i) $a > b$ and (ii) neither $(a, b, n) = (2, 1, 6)$ nor $a + b$ is a power of 2 and $n = 2$. Then, there exists a prime p such that $p \mid a^n - b^n$ and $p \nmid a^k - b^k$ for each positive integer $k < n$.*

Theorem 1.1 can be used to solve a generalization of Problem 1, for which we need to introduce some more notation.

Specifically, for $B, C \subseteq \mathbb{Z}$ we write $B \perp C$ if for every $b \in B$ there exists $c \in C$ such that $b \mid c$; this simplifies to $b \perp C$ when $B = \{b\}$. It is clear that $B \perp C$ if and only if $b \perp C$ for all $b \in B$.

Based on these premises, we then prove the following:

Theorem 1.3. *Pick $\varepsilon_0 \in \{\pm 1\}$ and let A be a set of prime powers with the property that $|A| \geq 3$ and $q \perp A$ whenever q is a prime dividing $\prod_{a \in B} a - \varepsilon_0$ for some $B \in \mathcal{P}_\star(A)$. Then, A is infinite. Also, $\mathbb{P} \perp A$ if $\varepsilon_0 = 1$. Finally, $A = \mathbb{P}$ if $A \subseteq \mathbb{P}$.*

Theorem 1.3 is proved in Section 4. Incidentally, the result gives a solution of Problem 1 in the special case where $\varepsilon_0 = 1$ and $A \subseteq \mathbb{P}$, while providing another proof, although overcomplicated, of the infinitude of primes.

The conclusions of Theorem 1.3 leads to the following:

Question 3. Let $\mathfrak{P}$ be an infinite set of primes. Does there exist a set of prime powers, say A, such that $q \perp A$ for some $q \in \mathbb{P}$ if and only if q is a prime divisor of $\prod_{a\in B} a + 1$ for some $B \in \mathcal{P}_\star(A)$ and $q \in \mathfrak{P}$? If not, what about a "non-trivial" characterization of those $\mathfrak{P}$ for which this happens?

Another question along the same lines is as follows:

Question 4. Let $\mathfrak{P}$ be an infinite set of primes and pick $\varepsilon_0 \in \{\pm 1\}$. Does there exist a set A of prime powers such that $q \in \mathfrak{P}$ if and only if q is a prime divisor of $\prod_{a\in B} a - \varepsilon_0$ for some $B \in \mathcal{P}_\star(A)$? If not, can we provide a "non-trivial" characterization of those $\mathfrak{P}$ for which this is true?

Both of these questions are almost completely open to us. Two related (but easier) questions are answered by Examples 2 and 3 in Section 4.

2. Preparations

Here below, we fix some more notation and prove a few preliminary lemmas related to Question 1 in its full generality (that is, the analysis is not restricted to the special cases covered by Theorem 1.1).

For any purpose it may serve, we recall from the introduction that, in our notation, $0 \in \mathbb{N}$ and $\emptyset, A \notin \mathcal{P}_\star(A)$ for any set A.

In the remainder of this section, we suppose that there exist an integer $n \ge 3$, a set $\mathfrak{P} = \{p_1, \dots, p_n\}$ of n primes, integral exponents $v_1, \dots, v_n \in \mathbb{N}^+$, a nonempty subfamily $\mathcal{D}$ of $\mathcal{P}_\star(S_n)$, and a map $\varepsilon : \mathcal{P}_\star(S_n) \to \{\pm 1\}$ such that $p_1 < \cdots < p_n$ and $q \in \mathfrak{P}$ whenever $q \in \mathbb{P}$ and q divides $\prod_{i\in I} p_i^{v_i} - \varepsilon_I$ for some $I \in \mathcal{D}$, where $\varepsilon_I := \varepsilon(I)$ for economy of notation.

Accordingly, we show that these assumptions lead to a contradiction if $\mathcal{D}$ contains some distinguished subsets of S_n and the restriction of ε to the subcollection of these sets, herein denoted by $\mathcal{D}_0$, is constant: This is especially the case when $\mathcal{D}_0 = \mathcal{P}_1(S_n) \cup \mathcal{P}_{n-2}(S_n) \cup \mathcal{P}_{n-1}(S_n)$.

We let $P := \prod_{i=1}^n p_i^{v_i}$ and $\mathcal{D}^{\rm op} := \{S_n \setminus I : I \in \mathcal{D}\}$, and then for each $I \in \mathcal{P}_\star(S_n)$ we define

$$P_I := \prod_{i\in I} p_i^{v_i}, \quad P_{-I} := P_{S_n\setminus I} \quad \text{and} \quad \varepsilon_{-I} := \varepsilon_{S_n\setminus I}$$

(notice that $P = P_I \cdot P_{-I}$). In particular, given $i \in S_n$ we write P_i for $P_{\{i\}}$ and P_{-i} for $P_{-\{i\}}$, but also ε_i for $\varepsilon_{\{i\}}$ and ε_{-i} for $\varepsilon_{-\{i\}}$.

It then follows from our assumptions that there are maps $\alpha_1, \dots, \alpha_n : \mathcal{P}_\star(S_n) \to \mathbb{N}$ such that

$$P_{-I} = \varepsilon_{-I} + \prod_{i\in I} p_i^{\alpha_{i,I}} \quad \text{for every } I \in \mathcal{D}^{\rm op}, \tag{1}$$

where $\alpha_{i,I} := \alpha_i(I)$. Thus, if there exists $i \in S_n$ such that $\{i\} \in \mathcal{D}^{\rm op}$ then

$$P_{-i} = p_i^{\alpha_i} + \varepsilon_{-i}, \quad \text{with} \quad \alpha_i := \alpha_{i,\{i\}} \in \mathbb{N}^+ \tag{2}$$

(of course, $\alpha_i \geq 1$ since $P_{-i} - \varepsilon_{-i} \geq 2 \cdot 3 - 1$). This in turn implies that

$$P = P_{I_1} \cdot \left(\varepsilon_{-I_1} + \prod_{i \in I_1} p_i^{\alpha_{i,I_1}} \right) = P_{I_2} \cdot \left(\varepsilon_{-I_2} + \prod_{i \in I_2} p_i^{\alpha_{i,I_2}} \right), \tag{3}$$

for all $I_1, I_2 \in \mathcal{D}^{\mathrm{op}}$, which specializes to:

$$P = p_{i_1}^{v_{i_1}} \cdot \left(p_{i_1}^{\alpha_{i_1}} + \varepsilon_{-i_1} \right) = p_{i_2}^{v_{i_2}} \cdot \left(p_{i_2}^{\alpha_{i_2}} + \varepsilon_{-i_2} \right) \tag{4}$$

for all $i_1, i_2 \in S_n$ such that $\{i_1\}, \{i_2\} \in \mathcal{D}^{\mathrm{op}}$.

We mention in this respect that, for any fixed integer $b \neq 0$ and any finite subset $\mathcal{S}$ of $\mathbb{P}$, the diophantine equation

$$A \cdot (a^{x_1} - a^{x_2}) = B \cdot (b^{y_1} - b^{y_2}) \tag{5}$$

has only finitely many solutions in *positive* integers $a, A, B, x_1, x_2, y_1, y_2$ for which a is a prime, $\gcd(Aa, Bb) = 1$, $x_1 \neq x_2$ and all the prime factors of AB belong to $\mathcal{S}$; see [6] and the references therein. It follows that our equation (4) has only finitely many possible scenarios for ε taking the constant value -1 in $\mathcal{D}$.

However, the methods used in [6] are not effective and, as far as we can tell, a list of all the solutions to equation (5) is not known, not even in the special case when $A = B = 1$ and $b = 2$. Furthermore, there does not seem to be any obvious way to adapt the proof of the main result in [6] to cover all of the cases resulting from equation (4).

With this in mind, and based on (1), our main hypothesis can be now restated as

$$\text{“}q \mid P_{-I} - \varepsilon_{-I} \text{ for some } q \in \mathbb{P} \text{ and } I \in \mathcal{D}^{\mathrm{op}} \text{ only if } q \in \mathfrak{P}\text{”}. \tag{6}$$

In addition, we can easily derive, using (3) and unique factorization, that

$$\text{“}q \mid \varepsilon_{-I} + \textstyle\prod_{i \in I} p_i^{\alpha_{i,I}} \text{ for some } q \in \mathbb{P} \text{ and } I \in \mathcal{D}^{\mathrm{op}} \text{ only if } q \in \mathfrak{P}\text{”}. \tag{7}$$

Both of (6) and (7) will be often referred to throughout the article. Lastly, we say that ε is *k-symmetric* for a certain $k \in \mathbb{N}^+$ if both of the following conditions hold:

$$\text{(i) } I \in \mathcal{D} \cap \mathcal{P}_k(S_n) \text{ only if } I \in \mathcal{D}^{\mathrm{op}}; \quad \text{(ii) } \varepsilon_I = \varepsilon_{-I} \text{ for all } I \in \mathcal{D} \cap \mathcal{P}_k(S_n).$$

With all this in hand, we are finally ready to prove a few preliminary results that will be used later, in Section 3, to establish our main theorem.

2.1. **Preliminaries.** The material is intentionally organized into a list of lemmas based on “local”, rather than “global”, hypotheses.

This is motivated by the idea of highlighting which is used for which purpose, in the hope that this can help find an approach to solve Question 1 in a broader generality.

In particular, the first half of Theorem 1.1, namely the one corresponding to the case $\varepsilon_0 = 1$, will be an immediate corollary of Lemma 2.6 below (the second part needs more work).

In what follows, given $a, b \in \mathbb{Z}$ with $a^2 + b^2 \neq 0$ we use $\gcd(a, b)$ for the greatest common divisor of a and b. Furthermore, for every $m \in \mathbb{N}^+$ such that $\gcd(a, m) = 1$ we denote by $\mathrm{ord}_m(a)$ the smallest $k \in \mathbb{N}^+$ for which $a^k \equiv 1 \bmod m$.

Lemma 2.1. *If $p_i = 3$ for some $i \in S_n$ and there exists $j \in S_n \setminus \{i\}$ such that $\{j\} \in \mathcal{D}^{\mathrm{op}}$, then one, and only one, of the following conditions holds:*

1. *$\varepsilon_{-j} = -1$ and α_j is even.*

2. $\varepsilon_{-j} = -1$, α_j *is odd and* $p_j \equiv 1 \bmod 6$.
3. $\varepsilon_{-j} = 1$, α_j *is odd and* $p_j \equiv 2 \bmod 3$.

Proof. The hypotheses and equation (4) give that $3 \mid p_j^{\alpha_j} + \varepsilon_{-j}$, which is possible only if one, and only one, of the desired conditions is satisfied. □

The next lemma, as elementary as it is, provides a sufficient condition under which $2 \in \mathfrak{P}$. (As a rule of thumb, having a way to show that 2 and 3 are in $\mathfrak{P}$ looks like a key aspect of the problem in its full generality.)

Lemma 2.2. *If there exists* $I \in \mathcal{D}$ *such that* $1 \notin I$ *then* $p_1 = 2$*; moreover,* $\alpha_1 \ge 4$ *if, in addition to the other assumptions,* $I \in \mathcal{P}_{n-1}(S_n)$.

Proof. Clearly, p_i is odd for each $i \in I$, which means that $P_I - \varepsilon_I$ is even, and hence $p_1 = 2$ by (6) and the assumed ordering of the primes p_i. Thus, it follows from (2) that if $I \in \mathcal{P}_{n-1}$ then $2^{\alpha_1} = P_{-1} - \varepsilon_{-1} \ge 3 \cdot 5 - 1$, with the result that $\alpha_1 \ge 4$. □

The following two lemmas prove that, in the case of a 1-symmetric ε, mild hypotheses imply that $3 \in \mathfrak{P}$.

Lemma 2.3. *Suppose that* ε *is* 1*-symmetric and pick a prime* $q \notin \mathfrak{P}$*. Then, there does not exist any* $i \in S_n$ *such that* $\{i\} \in \mathcal{D}$ *and* $p_i \equiv 1 \bmod q$.

Proof. Assume for the sake of contradiction that there exists $i_0 \in S_n$ such that $\{i_0\} \in \mathcal{D}$ and $p_{i_0} \equiv 1 \bmod q$. Then, using that ε is 1-symmetric, we get from (1) and (2) that

$$1 - \varepsilon_0 \equiv p_{i_0}^{v_{i_0}} - \varepsilon_0 \equiv \prod_{i \in I_0} p_i^{\alpha_{i,I_0}} \bmod q$$

and

$$P_{I_0} \equiv p_{i_0}^{\alpha_{i_0}} + \varepsilon_0 \equiv 1 + \varepsilon_0 \bmod q,$$

where $I_0 := S_n \setminus \{i_0\}$. But $q \notin \mathfrak{P}$ implies $q \nmid p_{i_0}^{v_{i_0}} - \varepsilon_0$ by (6), with the result that $\varepsilon_0 = -1$ (from the above), and then $q \mid P_{I_0}$.

By unique factorization, this is however in contradiction to the fact that q is not in $\mathfrak{P}$. □

Lemma 2.4. *Let* ε *be* 1*-symmetric and suppose there exists* $J \in \mathcal{P}_\star(S_n)$ *such that* $|S_n \setminus J|$ *is even,* $\mathcal{D}_0 := \mathcal{P}_1(S_n) \cup \{S_n \setminus J\} \subseteq \mathcal{D}$*, and the restriction of* ε *to* $\mathcal{D}_0$ *is constant. Then* $p_2 = 3$ *and* $\alpha_2 \ge \frac{1}{2}(5 - \varepsilon_0)$.

Proof. Let ε take the constant value ε_0 when restricted to $\mathcal{D}_0$ and assume by contradiction that $3 \notin \mathfrak{P}$.

Then, Lemma 2.3 gives that $p_i \equiv -1 \bmod 3$ for all $i \in S_n$, while taking $I = S_n \setminus \{i\}$ in (1) and working modulo 3 entails by (6) that

$$p_i^{v_i} - \varepsilon_0 \equiv \prod_{j \in I} p_j^{\alpha_{j,I}} \not\equiv 0 \bmod 3,$$

so that v_i is odd if $\varepsilon_0 = 1$ and even otherwise (here is where we use that $\mathcal{P}_1(S_n) \in \mathcal{D}$ and ε is 1-symmetric, in such a way that $\mathcal{P}_{n-1}(S_n) \in \mathcal{D}$ too). Now, since $S_n \setminus J \in \mathcal{D}$, the same kind of reasoning also yields that

$$1 - \varepsilon_0 \equiv P_{-J} - \varepsilon_0 \equiv \prod_{j \in J} p_j^{\alpha_{j,J}} \bmod 3,$$

with the result that if $\varepsilon_0 = 1$ then $3 \in \mathfrak{P}$ by (6), as follows from the fact that $S_n \setminus J$ has an even number of elements and v_i is odd for each $i \in J$ (which was proved before). This is however a contradiction.

So we are left with the case $\varepsilon_0 = -1$. Since -1 is not a quadratic residue modulo a prime $p \equiv -1 \bmod 4$, we get from the above and (2) that in this case $p_i \equiv 1 \bmod 4$ for each $i = 2, \dots, n$.

Therefore, (1) together with Lemma 2.2 gives that $P_{-1} + 1 = 2^{\alpha_1}$ with $\alpha_1 \geq 2$, which is again a contradiction as it means that $2 \equiv 0 \bmod 4$.

All of this proves that $p_2 = 3$, which in turn implies from (2) that $3^{\alpha_2} = P_{-2} - \varepsilon_{-2} \geq 2 \cdot 5 - \varepsilon_0$ (since ε is 1-symmetric and its restriction to $\mathcal{D}_0$ is constantly equal to ε_0, we have $\varepsilon_{-2} = \varepsilon_0$), so $\alpha_2 \geq 2$ if $\varepsilon_0 = 1$ and $\alpha_2 \geq 3$ if $\varepsilon_0 = -1$, i.e., $\alpha_2 \geq \frac{1}{2}(5 - \varepsilon_0)$ in both cases. □

We now show that, if $\mathcal{D}$ contains some distinguished subsets of S_n and ε is subjected to certain conditions, then p_i must be a Fermat prime.

Lemma 2.5. *Let $\mathcal{P}_1(S_n \setminus \{1\}) \subseteq \mathcal{D}^{\mathrm{op}}$ and assume there exists $i \in S_n \setminus \{1\}$ such that $\{i\} \in \mathcal{D}$ and $\varepsilon_{\pm i} = 1$. Then, p_i is a Fermat prime.*

Proof. It is clear from Lemma 2.2 that $p_1 = 2$. Suppose by contradiction that there exists an odd prime q such that $q \mid p_i - 1$ (note that $p_i \geq 3$), and hence $q \mid p_i^{v_i} - \varepsilon_i$.

Then, taking $I = \{i\}$ in (6) gives that $q = p_j$ for some $j \in S_n \setminus \{1, i\}$. Considering that $\mathcal{P}_1(S_n \setminus \{1\}) \subseteq \mathcal{D}^{\mathrm{op}}$, it follows from (4) that

$$p_j^{v_j}(p_j^{\alpha_j} + \varepsilon_{-j}) = p_i^{v_i}(p_i^{\alpha_i} + 1),$$

where we use that $\varepsilon_{-i} = 1$. This is however a contradiction, because it implies that $0 \equiv 2 \bmod p_j$ (with $p_j \geq 3$). So, p_i is a Fermat prime by [7, Theorem 17]. □

Lemma 2.6. *Let $\mathcal{P}_1(S_n) \subseteq \mathcal{D}^{\mathrm{op}}$ and suppose that $p_i = 3$ for some $i \in S_n$ and there exists $j \in S_n \setminus \{1, i\}$ such that $\{j\} \in \mathcal{D}$ and $\varepsilon_{\pm j} = 1$. Then $i = 2$, $p_1 = 2$, and $\varepsilon_{-1} = -1$.*

Proof. First, we have by Lemma 2.2 that $p_1 = 2$, and hence $i = 2$. Also, p_j is a Fermat prime by Lemma 2.5 (and clearly $p_j \geq 5$). So assume for a contradiction that $\varepsilon_{-1} = 1$.

Then, Lemma 2.1 and (2) imply that $p_j \mid P_{-1} = 2^{\alpha_1} + 1$ with α_1 odd, with the result that $2 \leq \mathrm{ord}_{p_j}(2) \leq \gcd(2\alpha, p_j - 1) = 2$. It follows that $5 \leq p_j \leq 2^2 - 1$, which is obviously impossible. □

The proof of the next lemma depends on Zsigmondy's theorem. Although not strictly related to the statement and the assumptions of Theorem 1.1, it will be of great importance later on.

Lemma 2.7. *Pick $p, q \in \mathbb{P}$ and assume that there exist $x, y, z \in \mathbb{N}$ for which $x \neq 0$, $y \geq 2$, $p \mid q + 1$ and $q^x - 1 = p^y(q^z - 1)$. Then $x = 2$, $z = 1$, $p = 2$, $y \in \mathbb{P}$, and $q = 2^y - 1$.*

Proof. Since $x \neq 0$, it is clear that $q^x - 1 \neq 0$, with the result that $z \neq 0$ and $q^z - 1 \neq 0$ too. Therefore, using also that $y \neq 0$, one has that

$$p^y = (q^x - 1)/(q^z - 1) > 1, \tag{8}$$

which is obviously possible only if

$$x > z \geq 1. \tag{9}$$

We claim that $x \leq 2$. For suppose to the contrary that $x > 2$. Then by Zsigmondy's theorem, there must exist at least one $r \in \mathbb{P}$ such that $r \mid q^x - 1$ and

$$r \nmid q^k - 1 \text{ for each positive integer } k < x.$$

In particular, (8) yields that $r = p$ (by unique factorization), which is a contradiction since $p \mid q^2 - 1$. Thus, we get from (9) that $x = 2$ and $z = 1$. Then, $p^y = q + 1$, that is $p^y - 1 \in \mathbb{P}$, and this is absurd unless $p = 2$ and $y \in \mathbb{P}$. The claim follows. □

This completes the preliminaries, and we can now proceed to the proof of the main result of the paper.

3. Proof of Theorem 1.1

Throughout we use the same notation and assumptions as in Section 2, but we specialize to the case where

$$\mathcal{D}_0 := \mathcal{P}_1(S_n) \cup \mathcal{P}_{n-2}(S_n) \cup \mathcal{P}_{n-1}(S_n) \subseteq \mathcal{D}$$

and ε takes the constant value ε_0 when restricted to $\mathcal{D}_0$ (as in the statement of Theorem 1.1).

Proof of Theorem 1.1. At least one of $n-2$ or $n-1$ is even, so we have by Lemmas 2.2 and 2.4 that $p_1 = 2$, $p_2 = 3$ and $v_2 \geq 2$.

There is, in consequence, no loss of generality in assuming, as we do, that $\varepsilon_0 = -1$, since the other case is impossible by Lemma 2.6.

Thus, pick $i_0 \in S_n$ such that $3 \mid p_{i_0} + 1$. It follows from (3) and our hypotheses that there exist $\beta_{i_0}, \gamma_{i_0} \in \mathbb{N}$ such that

$$P = 3^{v_2}(3^{\alpha_2} - 1) = p_{i_0}^{v_{i_0}} \cdot \left(p_{i_0}^{\alpha_{i_0}} - 1\right) = 3^{v_2} p_{i_0}^{v_{i_0}} \cdot \left(3^{\beta_{i_0}} p_{i_0}^{\gamma_{i_0}} - 1\right),$$

with the result that, on the one hand,

$$p_{i_0}^{\alpha_{i_0}} - 1 = 3^{v_2} \cdot \left(3^{\beta_{i_0}} p_{i_0}^{\gamma_{i_0}} - 1\right), \tag{10}$$

and on the other hand,

$$3^{\alpha_2} - 1 = p_{i_0}^{v_{i_0}} \cdot \left(3^{\beta_{i_0}} p_{i_0}^{\gamma_{i_0}} - 1\right). \tag{11}$$

Then, since $v_2 \geq 2$ and $\alpha_{i_0} \neq 0$, we see by (10) and Lemma 2.7 that $\beta_{i_0} \geq 1$. It is then found from (11) that $-1 \equiv (-1)^{v_{i_0}+1} \bmod 3$, i.e., v_{i_0} is even. To wit, we have proved that

$$\forall i \in S_n : p_i \equiv -1 \bmod 3 \implies v_i \text{ is even and } p_i^{v_i} \equiv 1 \bmod 3. \tag{12}$$

But every prime $\neq 3$ is congruent to ± 1 modulo 3. Therefore, we get from (2) and (12) that

$$2 \equiv \prod_{i \in S_n \setminus \{2\}} p_i^{v_i} + 1 \equiv 3^{\alpha_2} \equiv 0 \bmod 3,$$

which is obviously a contradiction and completes the proof. □

4. Proof of Theorem 1.3

In the present section, unless differently specified, we use the same notation and assumptions of Theorem 1.3, whose proof is split into three lemmas (one for each aspect of the claim).

Lemma 4.1. *A is an infinite set.*

Proof. Suppose to a contradiction that A is finite and let $n := |A|$.

Since A is a set of prime powers, there then exist $p_1, \dots, p_n \in \mathbb{P}$ and $v_1, \dots, v_n \in \mathbb{N}^+$ such that $p_1 \leq \cdots \leq p_n$ and $A = \{p_1^{v_1}, \dots, p_n^{v_n}\}$, and our assumptions give that

$$\text{“}q \text{ divides } \textstyle\prod_{i\in I} p_i^{v_i} - \varepsilon_0 \text{ for some } I \in \mathcal{P}_\star(S_n) \text{ only if } q \in \mathfrak{P}\text{”}, \tag{13}$$

where $\mathfrak{P} := \{p_1, \dots, p_n\}$ for brevity's sake.

This clearly implies that $p_1 < \cdots < p_n$. In fact, if $p_{i_1} = p_{i_2}$ for distinct $i_1, i_2 \in S_n$, then it is found from (13) and unique factorization that

$$p_{i_1}^k = \prod_{i\in S_n\setminus\{i_1\}} p_i^{v_i} - \varepsilon_0$$

for a certain $k \in \mathbb{N}^+$, which is impossible when reduced modulo p_{i_1}.

Thus, using that $n \geq 3$, it follows from Theorem 1.1 that there also exists $q \in \mathbb{P} \setminus \mathfrak{P}$ such that q divides $\prod_{i\in I} p_i^{v_i} - \varepsilon_0$ for some $I \in \mathcal{P}_\star(S_n)$. This is, however, in contradiction to (13), and the proof is complete. □

Lemma 4.2. *If $\varepsilon_0 = 1$, then $\mathbb{P} \perp A$. In particular, $A = \mathbb{P}$ if $A \subseteq \mathbb{P}$.*

Proof. Suppose for the sake of contradiction that there exists $p \in \mathbb{P}$ such that p does not divide any element of A.

Since $|A| = \infty$ (by Lemma 4.1), this together with the pigeonhole principle implies that, for a certain $r \in S_{p-1}$, the set

$$A_r := \{a \in A : a \equiv r \bmod p\}$$

is infinite, and we have that

$$\forall B \in \mathcal{P}_\star(A_r) : \prod_{a\in B} a \equiv \prod_{a\in B} r \equiv r^{|B|} \bmod p. \tag{14}$$

As it is now possible to choose $B_0 \in \mathcal{P}_\star(A_r)$ in such a way that $|B_0|$ is a multiple of $p-1$, one gets from (14) and Fermat's little theorem that p divides a number of the form $\prod_{a\in B} a - 1$ for some $B \in \mathcal{P}_\star(A)$, and hence $p \mid a_0$ for some $a_0 \in A$ (by the assumptions of Theorem 1.3).

This is, however, absurd, because by construction no element of A is divisible by p. It follows that $\mathbb{P} \perp A$, and the rest is trivial. □

In the next lemma, we let an empty sum be equal to 0 and an empty product be equal to 1, as usual.

Lemma 4.3. *If $\varepsilon_0 = -1$ and $A \subseteq \mathbb{P}$, then $A = \mathbb{P}$.*

Proof. Suppose to a contradiction that there exists $p \in \mathbb{P}$ such that $p \notin A$, and for each $r \in S_{p-1}$ let $A_r := \{a \in A : a \equiv r \bmod p\}$. Then,

$$A = A_1 \cup \cdots \cup A_{p-1}. \tag{15}$$

In addition to this, set $\Gamma_{\text{fin}} := \{r \in S_{p-1} : |A_r| < \infty\}$ and $\Gamma_{\text{inf}} := S_{p-1} \setminus \Gamma_{\text{fin}}$, and take

$$A_{\text{fin}} := \bigcup_{r\in\Gamma_{\text{fin}}} A_r \quad \text{and} \quad A_{\text{inf}} := A \setminus A_{\text{fin}}.$$

It is clear from (15) that A_{inf} is infinite, because A_{fin} is finite, $\{A_{\text{fin}}, A_{\text{inf}}\}$ is a partition of A, and $|A| = \infty$ by Lemma 4.1. So, we let $\xi_0 := \prod_{a\in A_{\text{fin}}} a$.

We claim that there exists a sequence $\varrho_0, \varrho_1, \ldots$ of positive integers such that ϱ_n is, for each $n \in \mathbb{N}$, a nonempty product (of a finite number) of distinct elements of A with the property that

$$\xi_0 \mid \varrho_n \quad \text{and} \quad 1 + \varrho_n \equiv \sum_{i=0}^{n+1} \varrho_0^i \bmod p. \tag{16}$$

Proof of the claim. We construct the sequence $\varrho_0, \varrho_1, \ldots$ in a recursive way. To start with, pick an arbitrary $a_0 \in A_{\text{inf}}$ and define $\varrho_0 := a_0\xi_0$, where the factor a_0 accounts for the possibility that $\Gamma_{\text{fin}} = \emptyset$.

By construction, ϱ_0 is a nonempty product of distinct elements of A, and (16) is satisfied in the base case $n = 0$.

Now fix $n \in \mathbb{N}$ and suppose that we have already found $\varrho_n \in \mathbb{N}^+$ such that ϱ_n is a product of distinct elements of A and (16) holds true with ϱ_0 and ϱ_n. By unique factorization, there then exist exponents $s_1, \ldots, s_k \in \mathbb{N}^+$ and distinct primes $p_1, \ldots, p_k \in \mathbb{P}$ ($k \in \mathbb{N}^+$) such that

$$\xi_0 \mid \varrho_n \quad \text{and} \quad 1 + \varrho_n = \prod_{i=1}^{k} p_i^{s_i}. \tag{17}$$

Therefore, we get from the assumptions on A that $p_i \perp A$ for each $i \in S_k$, which in turn implies that $p_i \in A$ (since $A \subseteq \mathbb{P}$ by hypothesis), and actually $p_i \in A_{\text{inf}}$, considering that every element of A_{fin}, if any exists, is a divisor of ξ_0, and $\xi_0 \mid \varrho_n$ by (17).

Using that A_r is infinite for every $r \in \Gamma_{\text{inf}}$ and $A_{\text{inf}} = \bigcup_{r\in\Gamma_{\text{inf}}} A_r$, this yields that there exist $a_1, \ldots, a_h \in A_{\text{inf}}$ such that, on the one hand,

$$\varrho_0 < a_1 < \cdots < a_h, \tag{18}$$

and on the other hand,

$$p_i \equiv a_{1+t_i} \equiv \cdots \equiv a_{s_i+t_i} \bmod p \tag{19}$$

for every $i \in S_k$, where we define $h := \sum_{i=1}^{k} s_i$ and $t_i := \sum_{j=1}^{i-1} s_j$. It follows from (17) and (19) that

$$1 + \varrho_n \equiv \prod_{i=1}^{k} p_i^{s_i} \equiv \prod_{i=1}^{h} a_i \bmod p.$$

So, by the assumptions on ϱ_n and the above considerations, we see that

$$1 + \varrho_0 \cdot \prod_{i=1}^{h} a_i \equiv 1 + \varrho_0 \cdot (1 + \varrho_n) \equiv 1 + \varrho_0 \cdot \sum_{i=0}^{n+1} \varrho_0^i \equiv \sum_{i=0}^{n+2} \varrho_0^i \bmod p.$$

Our claim is hence proved (by induction) by taking $\varrho_{n+1} := \varrho_0 \cdot \prod_{i=1}^{h} a_i$, because $\xi_0 \mid \varrho_0 \mid \varrho_{n+1}$ and ϱ_{n+1} is, by virtue of (18), a nonempty product of distinct elements of A. □

Thus, letting $n = p(p-1)-2$ in (16) and observing that $p \nmid \varrho_0$ (since $p \notin A$ and ϱ_0 is, by construction, a product of elements of A) give that $1+\varrho_n \equiv 0 \bmod p$, with the result that $p \in A$ by the assumed properties of A. This is, however, a contradiction, and the proof is complete. □

Finally, we have all the ingredients for the following:

Proof of Theorem 1.3. Just put together Lemmas 4.1, 4.2 and 4.3. □

We conclude the section with a couple of examples, the first of which provides evidence of a substantial difference between Lemmas 4.2 and 4.3, and is potentially of interest in relation to Question 3.

Example 2. Given $\ell \in \mathbb{N}^+$ and odd primes $q_1, \dots, q_\ell$, let

$$k := \operatorname{lcm}(q_1 - 1, \dots, q_\ell - 1)$$

and

$$A := \{p^{nk} : p \in \mathbb{P} \setminus \mathcal{Q}, n \in \mathbb{N}^+\},$$

where $\mathcal{Q} := \{q_1, \dots, q_\ell\}$. We denote by $\mathfrak{P}$ the set of all primes q for which there exists $B \in \mathcal{P}_\star(A)$ such that q divides $\prod_{a\in B} a + 1$.

It is then easily seen that $\mathfrak{P} \subseteq \mathbb{P} \setminus \mathcal{Q}$, since for every $B \in \mathcal{P}_\star(A)$ and each $i = 1, \dots, \ell$ Fermat's little theorem gives $\prod_{a\in B} a + 1 \equiv 2 \not\equiv 0 \bmod q_i$.

On the other hand, the very definition of A yields that $q \perp A$, for some $q \in \mathbb{P}$, if and only if $q \notin \mathcal{Q}$.

The example above shows that, given a finite nonempty $\mathcal{Q} \subseteq \mathbb{P}$, there exists a set A of prime powers such that the set of primes dividing at least one number of the form $\prod_{a\in B} a + 1$ for some $B \in \mathcal{P}_\star(A)$ is contained in $\mathbb{P} \setminus \mathcal{Q}$, and Question 3 asks if this inclusion can be actually made into an equality for a suitable A.

The next example, on the other hand, may be of interest in relation to Question 4.

Example 3. For $\ell \in \mathbb{N}^+$ pick distinct primes $q_1, \dots, q_\ell \geq 3$ and, in view of [7, Theorem 110], let g_i be a primitive root modulo q_i.

A standard argument based on the Chinese remainder theorem shows that there also exists an integer g such that g is a primitive root modulo q_i for each i, and by Dirichlet's theorem on arithmetic progressions we can choose g to be prime. Now, fix $\varepsilon_0 \in \{\pm 1\}$ and define

$$A := \begin{cases} \bigcup_{i=1}^{\ell} \{g^{(q_i-1)n} : n \in \mathbb{N}^+\} & \text{if } \varepsilon_0 = 1 \\ \bigcup_{i=1}^{\ell} \{g^{\frac{1}{2}(q_i-1)(2n-1)} : n \in \mathbb{N}^+\} & \text{if } \varepsilon_0 = -1 \end{cases}.$$

If $\mathfrak{P}$ is the set of all primes q such that q divides $\prod_{a\in B} a - \varepsilon_0$ for some $B \in \mathcal{P}_\star(A)$, then on the one hand, $q_i \in \mathfrak{P}$ for each i (essentially by construction), and on the other hand, no element of A is divided by q_i (because g and q_i are coprime).

5. Closing remarks

Many "natural" questions related to the ones already stated in the previous sections arise, and perhaps it can be interesting to find them an answer.

Here are some examples: Is it possible to prove Theorem 1.1 under the weaker assumption that $\mathcal{D}_0$, as there defined, is $\mathcal{P}_1(S_n) \cup \mathcal{P}_{n-1}(S_n)$ instead of $\mathcal{P}_1(S_n) \cup \mathcal{P}_{n-2}(S_n) \cup \mathcal{P}_{n-1}(S_n)$? This is clearly the case if $n = 3$, but what about $n \ge 4$? And what if n is sufficiently large and $\mathcal{D}_0 = \mathcal{P}_k(S_n)$ for some $k \in S_n$? The answer to the latter question is negative for $k = 1$ (for, take $p_1, \dots, p_n$ to be the n smallest primes and let $v_1 = \cdots = v_n = \varepsilon_0 = 1$, then observe that, for each $i \in S_n$, the greatest prime divisor of $p_i^{v_i} - \varepsilon_0$ is $\le p_i - 1$). But what if $k \ge 2$?

In addition to the above: To what degree can the results of Section 2 be extended in the direction of Question 2? It seems worth mentioning in this respect that Question 2 has the following "abstract" formulation (we refer to [10, Ch. 1] for background on divisibility and related topics in the general theory of rings):

Question 5. Given an integral domain $\mathbb{F}$ and an integer $n \ge 3$, pick pairwise coprime non-units $u_1, \dots, u_n \in \mathbb{F}$ (assuming that this is actually possible), and let $\mathcal{D}$ be a nonempty subfamily of $\mathcal{P}_\star(S_n)$ with "enough" elements. Does there exist at least one irreducible $q \in \mathbb{F}$ such that q divides $\prod_{i \in I} u_i - 1$ for some $I \in \mathcal{D}$ and $q \nmid u_1 \cdots u_n$?

In the above, the condition that $u_1, \dots, u_n$ are non-units is necessary to ensure that $\prod_{i \in I} u_i - 1 \ne 0$ for each $I \in \mathcal{D}$ (otherwise the question would be, in a certain sense, trivial).

In fact, one may want to assume that $\mathbb{F}$ is a UFD, in such a way that an element is irreducible if and only if it is prime [10, Theorems 1.1 and 1.2]. In particular, it seems interesting to try to answer Question 5 in the special case where $\mathbb{F}$ is the ring of integers of a quadratic extension of $\mathbb{Q}$ with the property of unique factorization, and $u_1, \dots, u_n$ are primes in $\mathbb{F}$. Hopefully, this will be the subject of future work.

Acknowledgments

We are grateful to Carlo Pagano (Università di Roma Tor Vergata) for having suggested the key idea used in the proof of Lemma 4.3, to Alain Plagne (École Polytechnique) for remarks that improved the readability of the paper, and to anonymous referees for helpful comments.

The second named author was supported, during the preparation of the manuscript, by the European Community's 7th Framework Programme (FP7/2007-2013) under Grant Agreement No. 276487 (project ApProCEM), and partly from the ANR Project No. ANR-12-BS01-0011 (project CAESAR).

References

[1] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*. 4th ed., Springer, 2010.

[2] M. Becheanu, M. Andronache, M. Bălună, R. Gologan, D. Şerbănescu, and V. Vornicu, *Romanian Mathematical Competitions 2003*. Societatea de Ştiinţe Matematice din România, 2003.

[3] A. R. Booker, *On Mullin's second sequence of primes*. Integers **A12** (2012), #A4.

[4] D. Borwein, J. M. Borwein, P. B. Borwein, and R. Girgensohn, *Giuga's conjecture on primality*. Amer. Math. Monthly **103** (1996), 40–50.

[5] L. Brenton and A. Vasiliu, *Znám's problem*. Math. Mag. **75**, No. 1 (2002), 3–11.
[6] Y. Bugeaud and F. Luca, *On Pillai's Diophantine equation*. New York J. Math. **12** (2006), 193–217.
[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. 6th ed. (revised by D.R. Heath-Brown and J.H. Silverman), Oxford University Press, 2008.
[8] J. C. Lagarias, *Cyclic systems of simultaneous congruences*. Int. J. Number Theory **6**, No. 2 (2010), 219–245.
[9] F. Luca, *On the diophantine equation* $p^{x_1} - p^{x_2} = q^{y_1} - q^{y_2}$. Indag. Mathem. (N.S.) **14**, No. 2 (2003), 207–222.
[10] R. A. Mollin, *Algebraic Number Theory*. Discrete Mathematics and Its Applications, 2nd ed., Chapman and Hall/CRC, 2011.
[11] A. A. Mullin, *Recursive function theory (a modern look at a Euclidean idea)*. Bull. Amer. Math. Soc. **69** (1963), 737.
[12] W. Narkiewicz, *The Development of Prime Number Theory*. Springer-Verlag, 2000.
[13] K. Zsigmondy, *Zur Theorie der Potenzreste*. Monatsh. Math. **3**, No. 1 (1892), 265–284.

Università Bocconi, via Sarfatti 25, 20100 Milan, Italy.
E-mail address: leonetti.paolo@gmail.com

Laboratoire Jacques-Louis Lions (LJLL), Université Pierre et Marie Curie (UPMC), 4 place Jussieu, boîte courrier 187, 75252 Paris (cedex 05), France.
E-mail address: tringali@ann.jussieu.fr
URL: http://www.math.polytechnique.fr/~tringali/