Article

Not peer-reviewed version

A Common Approach to Three Open Problems in Number Theory

Apoloniusz Tyszka *

Posted Date: 18 May 2023

doi: 10.20944/preprints202303.0420.v7

Keywords: Brocard's problem; Brocard-Ramanujan equation x!+1=y^2; composite Fermat numbers; composite numbers of the form 2^(2^n)+1; Erd\"os' equation x(x+1)=y!

Article

A Common Approach to Three Open Problems in Number Theory

Apoloniusz Tyszka

University of Agriculture, Faculty of Production and Power Engineering, Balicka 116B, 30-149 Kraków, Poland; rttyszka@cyf-kr.edu.pl

Abstract: The following system of equations $\{x_1 \cdot x_1 = x_2,\ x_2 \cdot x_2 = x_3,\ 2^{2^{x_1}} = x_3,\ x_4 \cdot x_5 = x_2,\ x_6 \cdot x_7 = x_2\}$ has exactly one solution in $(\mathbb{N} \setminus \{0,1\})^7$, namely $(2,4,16,2,2,2,2)$. Conjecture 1 states that if a system of equations $\mathcal{S} \subseteq \{x_i \cdot x_j = x_k : i,j,k \in \{1,\ldots,7\}\} \cup \{2^{2^{x_j}} = x_k : j,k \in \{1,\ldots,7\}\}$ has at most five equations and at most finitely many solutions in $(\mathbb{N} \setminus \{0,1\})^7$, then each such solution $(x_1,\ldots,x_7)$ satisfies $x_1,\ldots,x_7 \leqslant 16$. Conjecture 1 implies that there are infinitely many composite numbers of the form $2^{2^n}+1$. Conjectures 3 and 5 are of similar kind. Conjecture 3 implies that if the equation $x!+1=y^2$ has at most finitely many solutions in positive integers x and y, then each such solution (x,y) belongs to the set $\{(4,5),(5,11),(7,71)\}$. Conjecture 5 implies that if the equation $x(x+1)=y!$ has at most finitely many solutions in positive integers x and y, then each such solution (x,y) belongs to the set $\{(1,2),(2,3)\}$. We describe semi-algorithms $\mathtt{sem}_j$ $(j=1,2,3)$ that never terminate. For every $j \in \{1,2,3\}$, if Conjecture j is true, then $\mathtt{sem}_j$ endlessly prints consecutive positive integers starting from 1. For every $j \in \{1,2,3\}$, if Conjecture j is false, then $\mathtt{sem}_j$ prints a finite number (including zero) of consecutive positive integers starting from 1.

Keywords: Brocard's problem; Brocard-Ramanujan equation $x!+1=y^2$; composite Fermat numbers; composite numbers of the form $2^{2^n}+1$; Erdös' equation $x(x+1)=y!$

MSC: 11D61; 11D85

---

1. Epistemic Notions Increase the Scope of Mathematics

Nicolas D. Goodman observed that epistemic notions increase the scope of mathematics, see [1]. For many finite sets $\mathcal{X} \subseteq \mathbb{N}^m$, we know an algorithm that decides $\mathcal{X}$ although no known algorithm computes a positive integer n satisfying $\mathcal{X} \subseteq [0,n]^m$. This holds as for many Diophantine equations the number of rational solutions is finite by applying Faltings' theorem. Faltings' theorem tell us that certain curves have at most finitely many rational points, but no known proof gives any bound on the sizes of the numerators and denominators of the coordinates of those points.

In Sections 2–4, our knowledge (including conjectures) about the set $\mathcal{X}$ is different. The considerations in Section 2 imply the existence of the set $\mathcal{X}_2 \subseteq (\mathbb{N} \setminus \{0,1\})^7$ whose finiteness/infiniteness is unknown although we conjecture that $\mathrm{card}(\mathcal{X}_2) < \omega \Rightarrow \mathcal{X}_2 \subseteq [2,16]^7$. The considerations in Section 3 imply the existence of the set $\mathcal{X}_3 \subseteq (\mathbb{N} \setminus \{0\})^6$ whose finiteness/infiniteness is unknown although we conjecture that $\mathrm{card}(\mathcal{X}_3) < \omega \Rightarrow \mathcal{X}_3 \subseteq [1,(24!)!]^6$. The considerations in Section 4 imply the existence of the set $\mathcal{X}_4 \subseteq (\mathbb{N} \setminus \{0\})^6$ whose finiteness/infiniteness is unknown although we conjecture that $\mathrm{card}(\mathcal{X}_4) < \omega \Rightarrow \mathcal{X}_4 \subseteq [1,720!]^6$. For every $j \in \{2,3,4\}$, we know an algorithm that decides the set $\mathcal{X}_j$.

2. Composite Numbers of the Form $2^{2^n}+1$

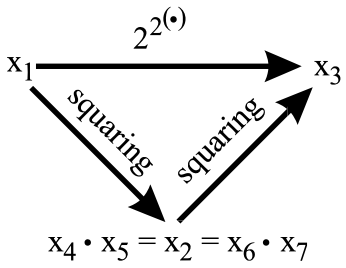
Let $\mathcal{A}$ denote the following system of equations:

$$\left\{x_i \cdot x_j = x_k :\ i,j,k \in \{1,\ldots,7\}\right\} \cup \left\{2^{2^{x_j}} = x_k :\ j,k \in \{1,\ldots,7\}\right\}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2023 doi:10.20944/preprints202303.0420.v7

The following subsystem of $\mathcal{A}$

$$\begin{cases} x_1 \cdot x_1 = x_2 \\ x_2 \cdot x_2 = x_3 \\ 2^{2^{x_1}} = x_3 \\ x_4 \cdot x_5 = x_2 \\ x_6 \cdot x_7 = x_2 \end{cases}$$



has exactly one solution in $(\mathbb{N} \setminus \{0,1\})^7$, namely $(2,4,16,2,2,2,2)$.

Conjecture 1. *If a system of equations $\mathcal{S} \subseteq \mathcal{A}$ has at most five equations and at most finitely many solutions in $(\mathbb{N} \setminus \{0,1\})^7$, then each such solution $(x_1, \ldots, x_7)$ satisfies $x_1, \ldots, x_7 \leqslant 16$.*

Lemma 1. *[[2] (p. 109)]. For every non-negative integers x and y, $x+1 = y$ if and only if $2^{2^x} \cdot 2^{2^x} = 2^{2^y}$.*

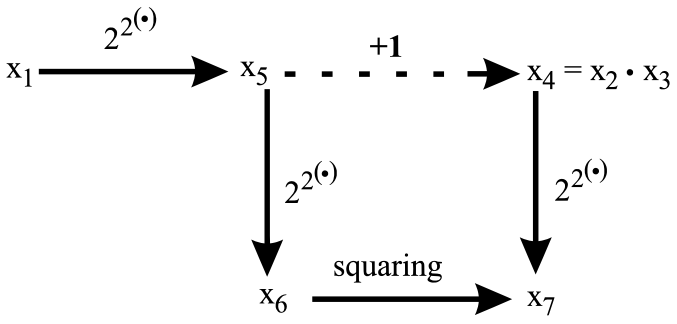
Theorem 2. *Conjecture 1 implies that $2^{2^{x_1}} + 1$ is composite for infinitely many integers x_1 greater than 1.*

Proof. Assume, on the contrary, that Conjecture 1 holds and $2^{2^{x_1}} + 1$ is composite for at most finitely many integers x_1 greater than 1. Then, the equation

$$x_2 \cdot x_3 = 2^{2^{x_1}} + 1$$

has at most finitely many solutions in $(\mathbb{N} \setminus \{0,1\})^3$. By Lemma 1, in positive integers greater than 1, the following subsystem of $\mathcal{A}$

$$\begin{cases} 2^{2^{x_1}} = x_5 \\ 2^{2^{x_5}} = x_6 \\ 2^{2^{x_4}} = x_7 \\ x_6 \cdot x_6 = x_7 \\ x_2 \cdot x_3 = x_4 \end{cases}$$



has at most finitely many solutions in $(\mathbb{N} \setminus \{0,1\})^7$ and expresses that

$$\begin{cases} x_2 \cdot x_3 = 2^{2^{x_1}} + 1 \\ x_4 = 2^{2^{x_1}} + 1 \\ x_5 = 2^{2^{x_1}} \\ x_6 = 2^{2^{2^{x_1}}} \\ x_7 = 2^{2^{2^{x_1}}} + 1 \end{cases}$$

Since $641 \cdot 6700417 = 2^{2^5} + 1 > 16$, we get a contradiction. □

Most mathematicians believe that $2^{2^n} + 1$ is composite for every integer $n \geqslant 5$, see [3, p. 23].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2023 doi:10.20944/preprints202303.0420.v7

Open Problem 1 ([4] (p. 159)). *Are there infinitely many composite numbers of the form* $2^{2^n}+1$*?*

Primes of the form $2^{2^n}+1$ are called Fermat primes, as Fermat conjectured that every integer of the form $2^{2^n}+1$ is prime, see [4] (p. 1). Fermat remarked that $2^{2^0}+1=3$, $2^{2^1}+1=5$, $2^{2^2}+1=17$, $2^{2^3}+1=257$, and $2^{2^4}+1=65537$ are all prime, see [4, p. 1].

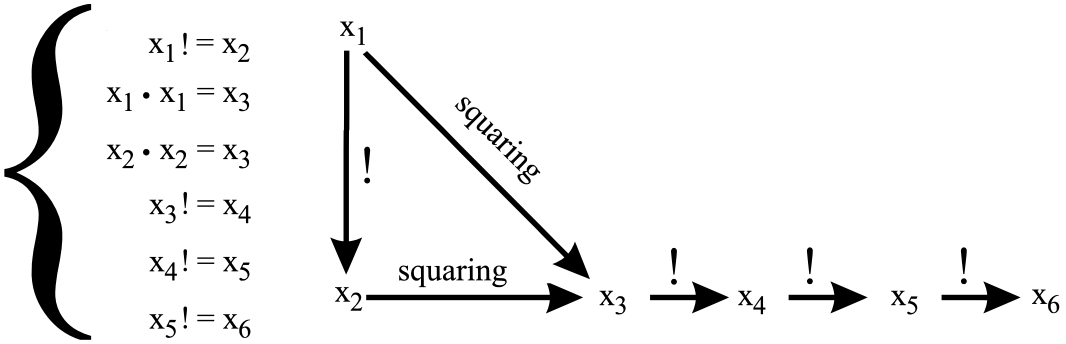
Open Problem 2 ([4] (p. 158)). *Are there infinitely many prime numbers of the form* $2^{2^n}+1$*?*

3. The Brocard-Ramanujan equation $x!+1=y^2$

Let $\mathcal{B}$ denote the following system of equations:

$$\{x_i \cdot x_j = x_k : i,j,k \in \{1,\dots,6\}\} \cup \{x_j! = x_k : (j,k \in \{1,\dots,6\}) \wedge (j \neq k)\}$$

The following subsystem of $\mathcal{B}$



has exactly two solutions in positive integers, namely $(1,\dots,1)$ and $(2,2,4,24,24!,(24!)!)$.

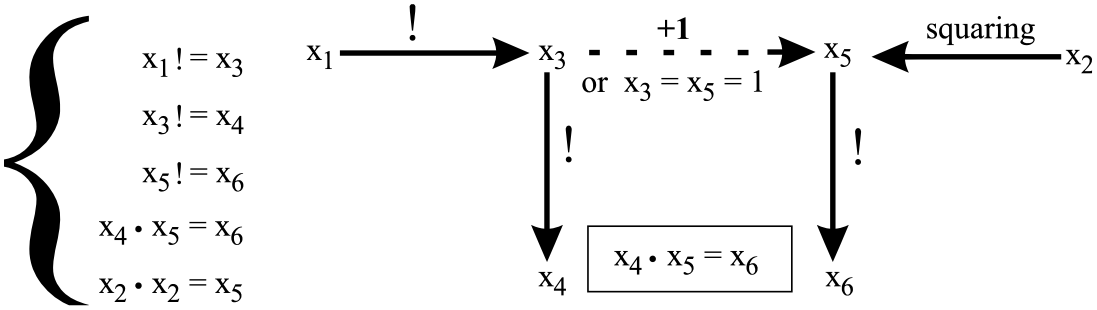
Conjecture 3. *If a system of equations* $\mathcal{S} \subseteq \mathcal{B}$ *has at most finitely many solutions in positive integers* $x_1,\dots,x_6$*, then each such solution* $(x_1,\dots,x_6)$ *satisfies* $x_1,\dots,x_6 \leqslant (24!)!$*.*

Lemma 2. *For every positive integers* x *and* y*,* $x! \cdot y = y!$ *if and only if*

$$(x+1=y) \vee (x=y=1)$$

Theorem 4. *Conjecture 3 implies that if the equation* $x_1!+1=x_2^2$ *has at most finitely many solutions in positive integers* x_1 *and* x_2*, then each such solution* (x_1,x_2) *belongs to the set* $\{(4,5),(5,11),(7,71)\}$*.*

Proof. The following system of equations $\mathcal{B}_1$



Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2023 doi:10.20944/preprints202303.0420.v7

is a subsystem of $\mathcal{B}$. By Lemma 2, in positive integers, the system $\mathcal{B}_1$ expresses that $x_1 = \ldots = x_6 = 1$ or

$$\begin{cases} x_1! + 1 &= x_2^2 \\ x_3 &= x_1! \\ x_4 &= (x_1!)! \\ x_5 &= x_1! + 1 \\ x_6 &= (x_1! + 1)! \end{cases}$$

If the equation $x_1! + 1 = x_2^2$ has at most finitely many solutions in positive integers x_1 and x_2, then $\mathcal{B}_1$ has at most finitely many solutions in positive integers $x_1, \ldots, x_6$ and Conjecture 3 implies that every tuple $(x_1, \ldots, x_6)$ of positive integers that solves $\mathcal{B}_1$ satisfies $(x_1! + 1)! = x_6 \leqslant (24!)!$. Hence, $x_1 \in \{1, \ldots, 23\}$. If $x_1 \in \{1, \ldots, 23\}$, then $x_1! + 1$ is a square only for $x_1 \in \{4, 5, 7\}$. □

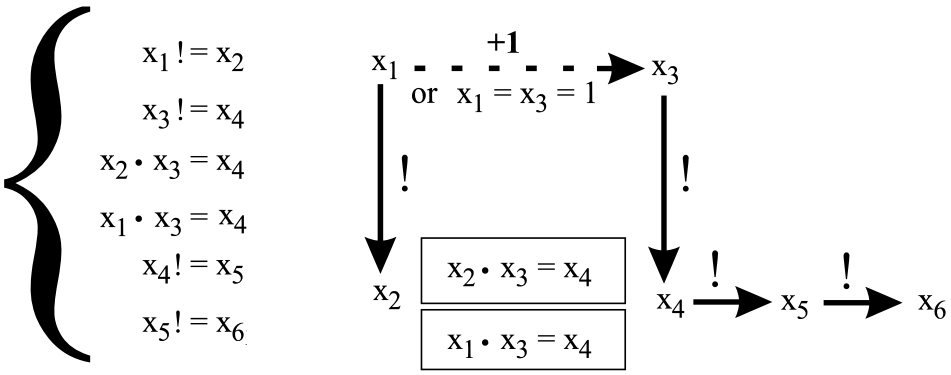
It is conjectured that $x! + 1$ is a square only for $x \in \{4, 5, 7\}$, see [8] (p. 297). A weak form of Szpiro's conjecture implies that the equation $x! + 1 = y^2$ has only finitely many solutions in positive integers, see [9].

4. Erdös' Equation $x(x+1) = y!$

Let $\mathcal{C}$ denote the following system of equations:

$$\{x_i \cdot x_j = x_k : (i, j, k \in \{1, \ldots, 6\}) \wedge (i \neq j)\} \cup \{x_j! = x_k : (j, k \in \{1, \ldots, 6\}) \wedge (j \neq k)\}$$

The following subsystem of $\mathcal{C}$



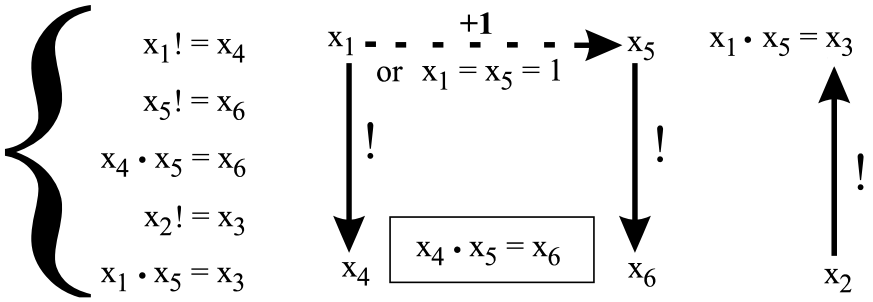
has exactly three solutions in positive integers, namely $(1, \ldots, 1)$, $(1, 1, 2, 2, 2, 2)$, and $(2, 2, 3, 6, 720, 720!)$.

Conjecture 5. *If a system of equations $\mathcal{S} \subseteq \mathcal{C}$ has at most finitely many solutions in positive integers $x_1, \ldots, x_6$, then each such solution $(x_1, \ldots, x_6)$ satisfies $x_1, \ldots, x_6 \leqslant 720!$.*

Theorem 6. *Conjecture 5 implies that if the equation $x_1(x_1 + 1) = x_2!$ has at most finitely many solutions in positive integers x_1 and x_2, then each such solution (x_1, x_2) belongs to the set $\{(1, 2), (2, 3)\}$.*

Proof. The following system of equations $\mathcal{C}_1$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2023 doi:10.20944/preprints202303.0420.v7



is a subsystem of $\mathcal{C}$. By Lemma 2, in positive integers, the system $\mathcal{C}_1$ expresses that $x_1 = \ldots = x_6 = 1$ or

$$\begin{cases} x_1 \cdot (x_1+1) &= x_2! \\ x_3 &= x_1 \cdot (x_1+1) \\ x_4 &= x_1! \\ x_5 &= x_1+1 \\ x_6 &= (x_1+1)! \end{cases}$$

If the equation $x_1(x_1+1) = x_2!$ has at most finitely many solutions in positive integers x_1 and x_2, then $\mathcal{C}_1$ has at most finitely many solutions in positive integers $x_1, \ldots, x_6$ and Conjecture 5 implies that every tuple $(x_1, \ldots, x_6)$ of positive integers that solves $\mathcal{C}_1$ satisfies $x_2! = x_3 \leqslant 720!$. Hence, $x_2 \in \{1, \ldots, 720\}$. If $x_2 \in \{1, \ldots, 720\}$, then $x_2!$ is a product of two consecutive positive integers only for $x_2 \in \{2, 3\}$ because the following *MuPAD* program

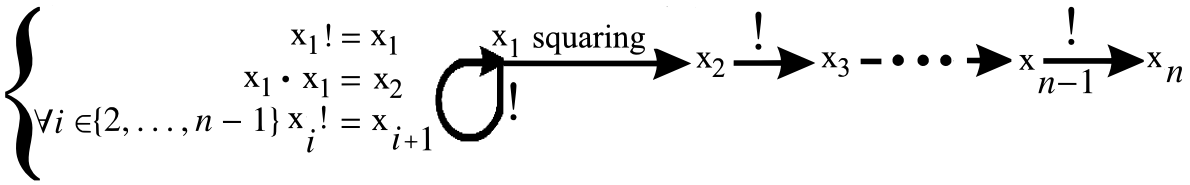
```
for x2 from 1 to 720 do
x1:=round(sqrt(x2!+(1/4))-(1/2)):
if x1*(x1+1)=x2! then print(x2) end_if:
end_for:
```

returns 2 and 3. □

The question of solving the equation $x(x+1) = y!$ was posed by P. Erdös, see [5]. F. Luca proved that the *abc* conjecture implies that the equation $x(x+1) = y!$ has only finitely many solutions in positive integers, see [6].

5. Conjectures 3 and 5 Cannot Be Generalized to An Arbitrary Number of Variables

Let $f(1) = 2$, $f(2) = 4$, and let $f(n+1) = f(n)!$ for every integer $n \geqslant 2$. Let $\mathcal{W}_1$ denote the system of equations $\{x_1! = x_1$. For an integer $n \geqslant 2$, let $\mathcal{W}_n$ denote the following system of equations:



For every positive integer n, the system $\mathcal{W}_n$ has exactly two solutions in positive integers $x_1, \ldots, x_n$, namely $(1, \ldots, 1)$ and $(f(1), \ldots, f(n))$. For a positive integer n, let Ψ_n denote the following statement: *if a system of equations*

$$\mathcal{S} \subseteq \{x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\} \cup \{x_j! = x_k : j, k \in \{1, \ldots, n\}\}$$

has at most finitely many solutions in positive integers $x_1, \ldots, x_n$, *then each such solution* $(x_1, \ldots, x_n)$ *satisfies* $x_1, \ldots, x_n \leqslant f(n)$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2023 doi:10.20944/preprints202303.0420.v7

Theorem 7. *Every factorial Diophantine equation can be algorithmically transformed into an equivalent system of equations of the forms $x_i \cdot x_j = x_k$ and $x_j! = x_k$. It means that this system of equations satisfies a modified version of Lemma 4 in [2].*

Proof. It follows from Lemmas 2–4 in [2] and Lemma 2. □

The statement $\forall n \in \mathbb{N} \setminus \{0\}\ \Psi_n$ is dubious. By Theorem 7, this statement implies that there is an algorithm which takes as input a factorial Diophantine equation and returns an integer which is greater than the solutions in positive integers, if these solutions form a finite set. This conclusion is strange because properties of factorial Diophantine equations are similar to properties of exponential Diophantine equations and a computable upper bound on non-negative integer solutions does not exist for exponential Diophantine equations with a finite number of solutions, see [7].

6. Equivalent Forms of Conjectures 1–5

If $k \in [10^{19}, 10^{20} - 1] \cap \mathbb{N}$, then there are uniquely determined non-negative integers $a(0), \ldots, a(19) \in \{0, \ldots, 9\}$ such that

$$\Big(a(19) \geqslant 1\Big) \wedge \Big(k = a(19) \cdot 10^{19} + a(18) \cdot 10^{18} + \ldots + a(1) \cdot 10^1 + a(0) \cdot 10^0\Big)$$

Definition 1. *For an integer $k \in [10^{19}, 10^{20} - 1]$, $\mathcal{S}_k$ stands for the smallest system of equations $\mathcal{S}$ satisfying conditions* `(1)` *and* `(2)`.

`(1)` *If $i \in \{0, 4, 8, 16\}$ and $a(i)$ is even, then the equation $x_{a(i+1)} \cdot x_{a(i+2)} = x_{a(i+3)}$ belongs to $\mathcal{S}$ when it belongs to $\mathcal{A}$.*

`(2)` *If $i \in \{0, 4, 8, 16\}$ and $a(i)$ is odd, then the equation $2^{2^{x_{a(i+1)}}} = x_{a(i+2)}$ belongs to $\mathcal{S}$ when it belongs to $\mathcal{A}$.*

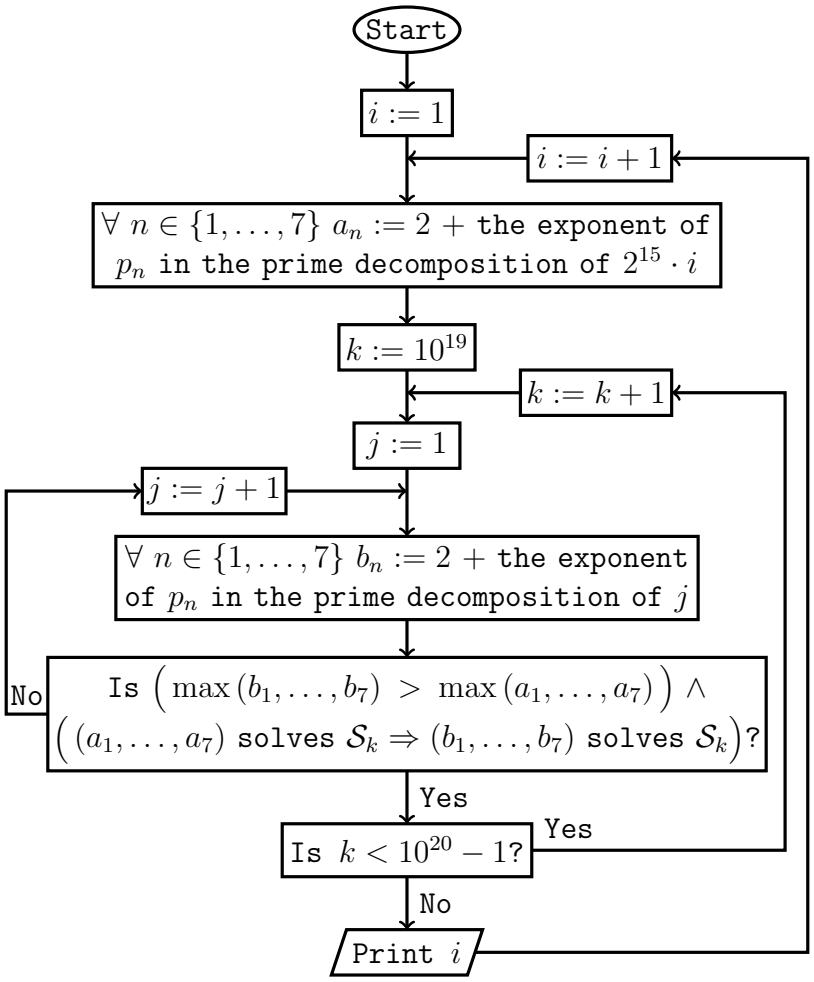
Lemma 3. $\{\mathcal{S}_k : k \in [10^{19}, 10^{20} - 1] \cap \mathbb{N} = \{\mathcal{S} : (\mathcal{S} \subseteq \mathcal{A}) \wedge (\mathrm{card}(\mathcal{S}) \leqslant 5)\}$.

Proof. It follows from the equality $5 \cdot 4 = 20$. □

For a positive integer n, let p_n denote the n-th prime number.

Theorem 8. *The following semi-algorithm* $\mathtt{sem}_1$ *never terminates.*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2023 doi:10.20944/preprints202303.0420.v7

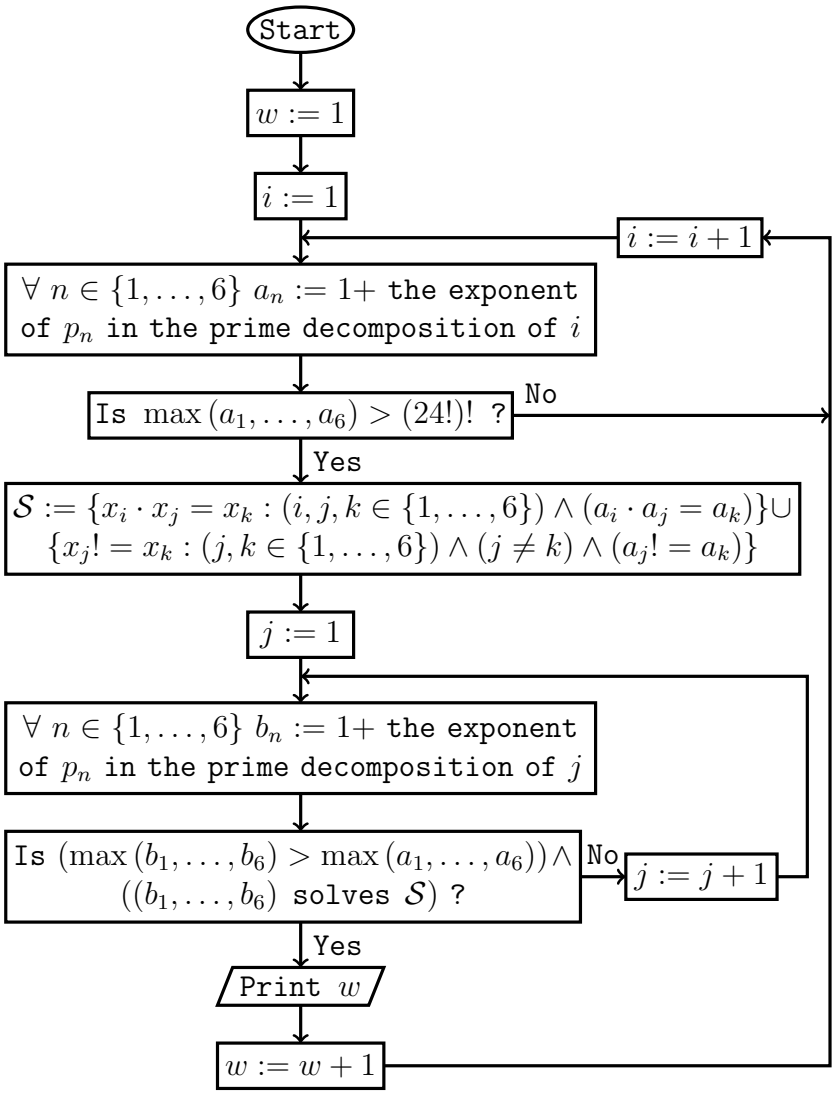


If Conjecture 1 is true, then $\texttt{sem}_1$ *endlessly prints consecutive positive integers starting from* 1. *If Conjecture 1 is false, then* $\texttt{sem}_1$ *prints a finite number (including zero) of consecutive positive integers starting from* 1.

Proof. It follows from Lemma 3. □

Theorem 9. *The following semi-algorithm* $\texttt{sem}_2$ *never terminates.*

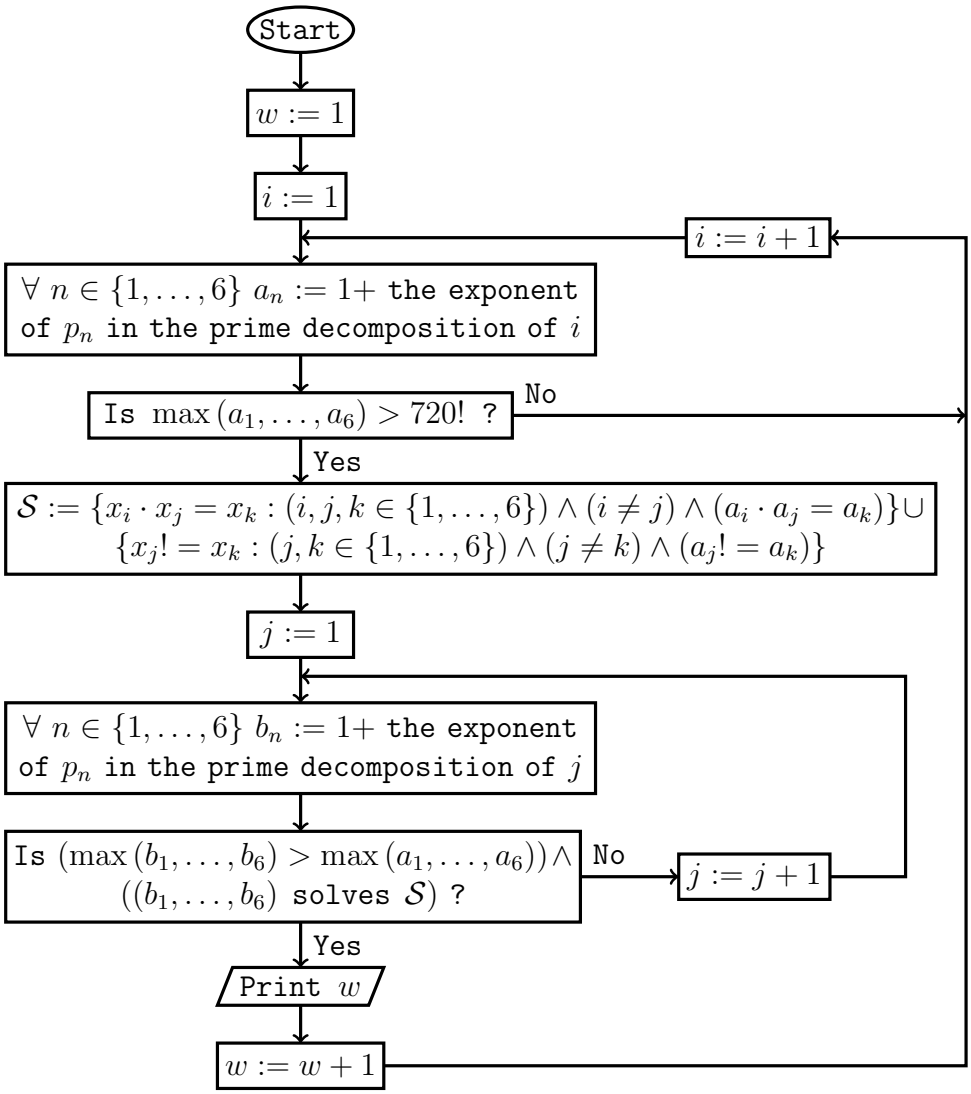
Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2023 doi:10.20944/preprints202303.0420.v7



If Conjecture 3 is true, then $\texttt{sem}_2$ *endlessly prints consecutive positive integers starting from* 1. *If Conjecture 3 is false, then* $\texttt{sem}_2$ *prints a finite number (including zero) of consecutive positive integers starting from* 1.

Theorem 10. *The following semi-algorithm* $\texttt{sem}_3$ *never terminates.*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2023 doi:10.20944/preprints202303.0420.v7



If Conjecture 5 is true, then $\texttt{sem}_3$ *endlessly prints consecutive positive integers starting from* 1. *If Conjecture 5 is false, then* $\texttt{sem}_3$ *prints a finite number (including zero) of consecutive positive integers starting from* 1.

References

1. N. D. Goodman, The Knowing Mathematician. *Synthese* **1984**, *60*, 21–38, Available online: http://link.springer.com/article/10.1007/BF00485616 Reprinted in: H. Leblanc, E. Mendelson, A. Orenstein, *Foundations: Logic, Language, and Mathematics*, Springer, 1984; pp. 21–38, Available online: http://link.springer.com/book/10.1007/978-94-017-1592-8.
2. A. Tyszka, A hypothetical upper bound on the heights of the solutions of a Diophantine equation with a finite number of solutions. *Open Comput. Sci.* **2018**, *8*, 109–114, http://doi.org/10.1515/comp-2018-0012.
3. J.-M. De Koninck and F. Luca. *Analytic Number Theory: Exploring the Anatomy of Integers*; American Mathematical Society: Providence, RI, 2012.
4. M. Křížek, F. Luca, L. Somer, *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, Springer: New York, 2001.
5. D. Berend and J. E. Harmse, *On polynomial-factorial Diophantine equations, Trans. Amer. Math. Soc.* **2006**, *358*, 1741–1779.
6. F. Luca, *The Diophantine equation* $P(x) = n!$ *and a result of M. Overholt, Glas. Mat. Ser. III* **2002**, *37*, 269–273.
7. Yu. Matiyasevich, Existence of noneffectivizable estimates in the theory of exponential Diophantine equations, *J. Sov. Math.* **1977**, *8*, 299–311, http://dx.doi.org/10.1007/bf01091549.

 doi:10.20944/preprints202303.0420.v7

8. E. W. Weisstein. *CRC Concise Encyclopedia of Mathematics*, 2nd ed., Chapman & Hall/CRC: Boca Raton, FL, 2002.
9. M. Overholt, The Diophantine equation $n! + 1 = m^2$, *Bull. London Math. Soc.* **1993**, *25*, 104.