A common approach to the problem of the infinitude of twin primes, primes of the form n!+1, and primes of the form n!-1

Apoloniusz Tyszka

A common approach to the problem of the infinitude of twin primes, primes of the form $n! + 1$, and primes of the form $n! - 1$

Apoloniusz Tyszka

Abstract

For a positive integer x, let $\Gamma(x)$ denote $(x-1)!$. Let $\text{fact}^{-1}\colon \{1,2,6,24,\ldots\} \to \mathbb{N} \setminus \{0\}$ denote the inverse function to the factorial function. For positive integers x and y, let $\text{rem}(x,y)$ denote the remainder from dividing x by y. For a positive integer n, by a computation of length n we understand any sequence of terms $x_1,\ldots,x_n$ such that x_1 is defined as the variable x, and for every integer $i \in \{2,\ldots,n\}$, x_i is defined as $\Gamma(x_{i-1})$, or $\text{fact}^{-1}(x_{i-1})$, or $\text{rem}(x_{i-1},x_{i-2})$ (only if $i \geqslant 3$ and x_{i-1} is defined as $\Gamma(x_{i-2})$). Let $f(4) = 3$, and let $f(n+1) = f(n)!$ for every integer $n \geqslant 4$. For an integer $n \geqslant 4$, let Ψ_n denote the following statement: if a computation of length n returns positive integers $x_1,\ldots,x_n$ for at most finitely many positive integers x, then every such x does not exceed $f(n)$. We prove: `(1)` the statement Ψ_4 equivalently expresses that there are infinitely many primes of the form $n! + 1$; `(2)` the statement Ψ_6 implies that for infinitely many primes p the number $p! + 1$ is prime; `(3)` the statement Ψ_6 implies that there are infinitely many primes of the form $n! - 1$; `(4)` the statement Ψ_7 implies that there are infinitely many twin primes.

2010 Mathematics Subject Classification: 11A41, 68Q05.

Key words and phrases: computation of length n, prime numbers of the form $n! + 1$, prime numbers of the form $n! - 1$, prime numbers p such that $p! + 1$ is prime, twin prime conjecture.

For a positive integer x, let $\Gamma(x)$ denote $(x-1)!$. Let $\text{fact}^{-1}\colon \{1,2,6,24,\ldots\} \to \mathbb{N} \setminus \{0\}$ denote the inverse function to the factorial function. For positive integers x and y, let $\text{rem}(x,y)$ denote the remainder from dividing x by y.

Definition. *For a positive integer n, by a computation of length n we understand any sequence of terms $x_1,\ldots,x_n$ such that x_1 is defined as the variable x, and for every integer $i \in \{2,\ldots,n\}$, x_i is defined as $\Gamma(x_{i-1})$, or $\text{fact}^{-1}(x_{i-1})$, or $\text{rem}(x_{i-1},x_{i-2})$ (only if $i \geqslant 3$ and x_{i-1} is defined as $\Gamma(x_{i-2})$).*

Let $f(4) = 3$, and let $f(n+1) = f(n)!$ for every integer $n \geqslant 4$. For an integer $n \geqslant 4$, let Ψ_n denote the following statement: if a computation of length n returns positive integers $x_1,\ldots,x_n$ for at most finitely many positive integers x, then every such x does not exceed $f(n)$.

Lemma 1. *For every positive integer n, there are only finitely many computations of length n.*

Theorem 1. *For every integer $n \geqslant 4$, the statement Ψ_n is true with an unknown integer bound that depends on n.*

Proof. It follows from Lemma 1. □

Let $\mathcal{P}$ denote the set of prime numbers.

Lemma 2. *([4, pp. 214–215]) . For every positive integer x, $\mathrm{rem}(\Gamma(x), x) \in \mathbb{N} \setminus \{0\}$ if and only if $x \in \{4\} \cup \mathcal{P}$.*

Theorem 2. *For every integer $n \geqslant 4$ and for every positive integer x, the following computation $\mathcal{H}$*

$$\begin{cases} x_1 := x \\ \forall i \in \{2, \ldots, n-3\}\ x_i := \mathrm{fact}^{-1}(x_{i-1}) \\ x_{n-2} := \Gamma(x_{n-3}) \\ x_{n-1} := \Gamma(x_{n-2}) \\ x_n := \mathrm{rem}(x_{n-1}, x_{n-2}) \end{cases}$$

returns positive integers $x_1, \ldots, x_n$ if and only if $x = f(n)$.

Proof. We make three observations.

Observation 1. *If $x_{n-3} = 3$, then $x_1, \ldots, x_{n-3} \in \mathbb{N} \setminus \{0\}$ and $x = x_1 = f(n)$.*
If $x = f(n)$, then $x_1, \ldots, x_{n-3} \in \mathbb{N} \setminus \{0\}$ and $x_{n-3} = 3$.
Hence, $x_{n-2} = \Gamma(x_{n-3}) = 2$ and $x_{n-1} = \Gamma(x_{n-2}) = 1$. Therefore, $x_n = \mathrm{rem}(x_{n-1}, x_{n-2}) = 1$.

Observation 2. *If $x_{n-3} = 2$, then $x = x_1 = \ldots = x_{n-3} = 2$.*
If $x = 2$, then $x_1 = \ldots = x_{n-3} = 2$. Hence, $x_{n-2} = \Gamma(x_{n-3}) = 1$ and $x_{n-1} = \Gamma(x_{n-2}) = 1$.
Therefore, $x_n = \mathrm{rem}(x_{n-1}, x_{n-2}) = 0 \notin \mathbb{N} \setminus \{0\}$.

Observation 3. *If $x_{n-3} = 1$, then $x_{n-2} = \Gamma(x_{n-3}) = 1$. Hence, $x_{n-1} = \Gamma(x_{n-2}) = 1$.*
Therefore, $x_n = \mathrm{rem}(x_{n-1}, x_{n-2}) = 0 \notin \mathbb{N} \setminus \{0\}$.

Observations 1–3 cover the case when $x_{n-3} \in \{1, 2, 3\}$. If $x_{n-3} \geqslant 4$, then $x_{n-2} = \Gamma(x_{n-3})$ is greater than 4 and composite. By Lemma 2, $x_n = \mathrm{rem}(x_{n-1}, x_{n-2}) = \mathrm{rem}(\Gamma(x_{n-2}), x_{n-2}) = 0 \notin \mathbb{N} \setminus \{0\}$. □

Corollary 1. *For every integer $n \geqslant 4$, the bound $f(n)$ in the statement Ψ_n cannot be decreased.*

Lemma 3. *(Wilson's theorem, [2, p. 89]). For every positive integer x, x divides $\Gamma(x) + 1$ if and only if $x \in \{1\} \cup \mathcal{P}$.*

Corollary 2. *If $x \in \mathcal{P}$, then $\mathrm{rem}(\Gamma(x), x) = x - 1$.*

Lemma 4. *For every positive integer x, the following computation $\mathcal{A}$*

$$\begin{cases} x_1 := x \\ x_2 := \Gamma(x_1) \\ x_3 := \mathrm{rem}(x_2, x_1) \\ x_4 := \mathrm{fact}^{-1}(x_3) \end{cases}$$

returns positive integers $x_1, \ldots, x_4$ if and only if $x = 4$ or x is a prime number of the form $n! + 1$.

Proof. For an integer $i \in \{1, \ldots, 4\}$, let A_i denote the set of positive integers x such that the first i instructions of the computation $\mathcal{A}$ returns positive integers $x_1, \ldots, x_i$. We show that

$$A_4 = \{4\} \cup (\{n! + 1 :\ n \in \mathbb{N} \setminus \{0\}\} \cap \mathcal{P}) \tag{1}$$

For every positive integer x, the terms x_1 and x_2 belong to $\mathbb{N} \setminus \{0\}$. By Lemma 2, the term x_3 (which equals $\mathrm{rem}(\Gamma(x), x)$) belongs to $\mathbb{N} \setminus \{0\}$ if and only if $x \in \{4\} \cup \mathcal{P}$. Hence, $A_3 = \{4\} \cup \mathcal{P}$. If $x = 4$, then $x_1, \ldots, x_4 \in \mathbb{N} \setminus \{0\}$. Hence, $4 \in A_4$. If $x \in \mathcal{P}$, then Corollary 2 implies that $x_3 = \mathrm{rem}(\Gamma(x), x) = x - 1 \in \mathbb{N} \setminus \{0\}$. Therefore, for every $x \in \mathcal{P}$, the term $x_4 = \mathrm{fact}^{-1}(x_3)$ belongs to $\mathbb{N} \setminus \{0\}$ if and only if $x \in \{n! + 1 :\ n \in \mathbb{N} \setminus \{0\}\}$. This proves equality (1). □

It is conjectured that there are infinitely many primes of the form $n! + 1$, see [1, p. 443] and [5].

Theorem 3. *The statement Ψ_4 implies that the set of primes of the form $n! + 1$ is infinite.*

Proof. The number $3! + 1 = 7$ is prime. By Lemma 4, for $x = 7$ the computation $\mathcal{A}$ returns positive integers $x_1, \ldots, x_4$. Since $x = 7 > 3 = f(4)$, the statement Ψ_4 guarantees that the computation $\mathcal{A}$ returns positive integers $x_1, \ldots, x_4$ for infinitely many positive integers x. By Lemma 4, there are infinitely many primes of the form $n! + 1$. □

Lemma 5. *If $x \in \mathbb{N} \setminus \{0, 1\}$, then $\mathrm{fact}^{-1}(\Gamma(x)) = x - 1$.*

Theorem 4. *If the set of primes of the form $n! + 1$ is infinite, then the statement Ψ_4 is true.*

Proof. There exist 10 computations of length 4 that differ from $\mathcal{H}$ and $\mathcal{A}$. We claim that every such computation $\mathcal{F}$ returns positive integers $x_1, \ldots, x_4$ for infinitely many positive integers x. We omit the easy proof (which uses Lemmas 2 and 5) as it is based on case analysis. □

Hypothesis. *The statements $\Psi_4, \ldots, \Psi_7$ are true.*

Lemma 6. *For every positive integer x, the following computation $\mathcal{B}$*

$$\begin{cases} x_1 := x \\ x_2 := \Gamma(x_1) \\ x_3 := \mathrm{rem}(x_2, x_1) \\ x_4 := \mathrm{fact}^{-1}(x_3) \\ x_5 := \Gamma(x_4) \\ x_6 := \mathrm{rem}(x_5, x_4) \end{cases}$$

returns positive integers $x_1, \ldots, x_6$ if and only if $x \in \{4\} \cup \{p! + 1 : \ p \in \mathcal{P}\} \cap \mathcal{P}$

Proof. For an integer $i \in \{1, \ldots, 6\}$, let B_i denote the set of positive integers x such that the first i instructions of the computation $\mathcal{B}$ returns positive integers $x_1, \ldots, x_i$. Since the computations $\mathcal{A}$ and $\mathcal{B}$ have the same first four instructions, the equality $B_i = A_i$ holds for every $i \in \{1, \ldots, 4\}$. In particular,

$$B_4 = \{4\} \cup (\{n! + 1 : \ n \in \mathbb{N} \setminus \{0\}\} \cap \mathcal{P})$$

We show that

$$B_6 = \{4\} \cup (\{p! + 1 : \ p \in \mathcal{P}\} \cap \mathcal{P}) \tag{2}$$

If $x = 4$, then $x_1, \ldots, x_6 \in \mathbb{N} \setminus \{0\}$. Hence, $4 \in B_6$. Let $x \in \mathcal{P}$, and let $x = n! + 1$, where $n \in \mathbb{N} \setminus \{0\}$. Hence, $n \neq 4$. Corollary 2 implies that $x_3 = \mathrm{rem}(\Gamma(x), x) = x - 1 = n!$. Hence, $x_4 = \mathrm{fact}^{-1}(x_3) = n$ and $x_5 = \Gamma(x_4) = \Gamma(n) \in \mathbb{N} \setminus \{0\}$. By Lemma 2, the term x_6 (which equals $\mathrm{rem}(\Gamma(n), n)$) belongs to $\mathbb{N} \setminus \{0\}$ if and only if $n \in \{4\} \cup \mathcal{P}$. This proves equality (2) as $n \neq 4$. □

Theorem 5. *The statement Ψ_6 implies that for infinitely many primes p the number $p! + 1$ is prime.*

Proof. The numbers 11 and $11! + 1$ are prime, see [1, p. 441] and [7]. By Lemma 6, for $x = 11! + 1$ the computation $\mathcal{B}$ returns positive integers $x_1, \ldots, x_6$. Since $x = 11! + 1 > 6! = f(6)$, the statement Ψ_6 guarantees that the computation $\mathcal{B}$ returns positive integers $x_1, \ldots, x_6$ for infinitely many positive integers x. By Lemma 6, for infinitely many primes p the number $p! + 1$ is prime. □

Lemma 7. *For every positive integer x, the following computation C*

$$\begin{cases} x_1 & := & x \\ x_2 & := & \Gamma(x_1) \\ x_3 & := & \Gamma(x_2) \\ x_4 & := & \mathrm{fact}^{-1}(x_3) \\ x_5 & := & \Gamma(x_4) \\ x_6 & := & \mathrm{rem}(x_5, x_4) \end{cases}$$

returns positive integers $x_1, \ldots, x_6$ if and only if $(x-1)! - 1$ is prime.

Proof. For an integer $i \in \{1, \ldots, 6\}$, let C_i denote the set of positive integers x such that the first i instructions of the computation C returns positive integers $x_1, \ldots, x_i$. If $x \in \{1, 2, 3\}$, then $x_6 = 0$. Therefore, $C_6 \subseteq \mathbb{N} \setminus \{0, 1, 2, 3\}$. By Lemma 5, for every integer $x \geqslant 4$, $x_4 = (x-1)! - 1$, $x_5 = \Gamma((x-1)! - 1)$, and $x_1, \ldots, x_5 \in \mathbb{N} \setminus \{0\}$. By Lemma 2, for every integer $x \geqslant 4$,

$$x_6 = \mathrm{rem}(\Gamma((x-1)! - 1), (x-1)! - 1)$$

belongs to $\mathbb{N} \setminus \{0\}$ if and only if $(x-1)! - 1 \in \{4\} \cup \mathcal{P}$. The last condition equivalently expresses that $(x-1)! - 1$ is prime as $(x-1)! - 1 \geqslant 5$ for every integer $x \geqslant 4$. Hence,

$$C_6 = (\mathbb{N} \setminus \{0, 1, 2, 3\}) \cap \{x \in \mathbb{N} \setminus \{0, 1, 2, 3\} : \ (x-1)! - 1 \in \mathcal{P}\} = \{x \in \mathbb{N} \setminus \{0\} : \ (x-1)! - 1 \in \mathcal{P}\}$$

□

It is conjectured that there are infinitely many primes of the form $n! - 1$, see [1, p. 443] and [6].

Theorem 6. *The statement Ψ_6 implies that there are infinitely many primes of the form $x! - 1$.*

Proof. The number $(975-1)! - 1$ is prime, see [1, p. 441] and [6]. By Lemma 7, for $x = 975$ the computation C returns positive integers $x_1, \ldots, x_6$. Since $x = 975 > 720 = f(6)$, the statement Ψ_6 guarantees that the computation C returns positive integers $x_1, \ldots, x_6$ for infinitely many positive integers x. By Lemma 7, the set $\{x \in \mathbb{N} \setminus \{0\} : \ (x-1)! - 1 \in \mathcal{P})\}$ is infinite. □

Lemma 8. *For every positive integer x, the following computation $\mathcal{D}$*

$$\begin{cases} x_1 & := & x \\ x_2 & := & \Gamma(x_1) \\ x_3 & := & \mathrm{rem}(x_2, x_1) \\ x_4 & := & \Gamma(x_3) \\ x_5 & := & \mathrm{fact}^{-1}(x_4) \\ x_6 & := & \Gamma(x_5) \\ x_7 & := & \mathrm{rem}(x_6, x_5) \end{cases}$$

returns positive integers $x_1, \ldots, x_7$ if and only if both x and $x-2$ are prime.

Proof. For an integer $i \in \{1, \ldots, 7\}$, let D_i denote the set of positive integers x such that the first i instructions of the computation $\mathcal{D}$ returns positive integers $x_1, \ldots, x_i$. If $x = 1$, then $x_3 = 0$. Hence, $D_7 \subseteq D_3 \subseteq \mathbb{N} \setminus \{0, 1\}$. If $x \in \{2, 3, 4\}$, then $x_7 = 0$. Therefore,

$$D_7 \subseteq (\mathbb{N} \setminus \{0, 1\}) \cap (\mathbb{N} \setminus \{0, 2, 3, 4\}) = \mathbb{N} \setminus \{0, 1, 2, 3, 4\}$$

By Lemma 2, for every integer $x \geqslant 5$, the term x_3 (which equals $\mathrm{rem}(\Gamma(x), x)$) belongs to $\mathbb{N} \setminus \{0\}$ if and only if $x \in \mathcal{P} \setminus \{2, 3\}$. By Corollary 2, for every $x \in \mathcal{P} \setminus \{2, 3\}$, $x_3 = x - 1 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$. By Lemma 5, for every $x \in \mathcal{P} \setminus \{2, 3\}$, the terms x_4 and x_5 belong to $\mathbb{N} \setminus \{0\}$ and $x_5 = x_3 - 1 = x - 2$. By Lemma 2, for every $x \in \mathcal{P} \setminus \{2, 3\}$, the term x_7 (which equals $\mathrm{rem}(\Gamma(x_5), x_5)$) belongs to $\mathbb{N} \setminus \{0\}$ if and only if $x_5 = x - 2 \in \{4\} \cup \mathcal{P}$. From these facts, we obtain that

$$D_7 = (\mathbb{N} \setminus \{0, 1, 2, 3, 4\}) \cap (\mathcal{P} \setminus \{2, 3\}) \cap (\{6\} \cup \{p + 2 : \ p \in \mathcal{P}\}) = \{p \in \mathcal{P} : \ p - 2 \in \mathcal{P}\}$$

□

A twin prime is a prime number that is either 2 less or 2 more than another prime number. The twin prime conjecture states that there are infinitely many twin primes, see [3, p. 39].

Theorem 7. *The statement Ψ_7 implies that there are infinitely many twin primes.*

Proof. Harvey Dubner proved that the numbers $459 \cdot 2^{8529} - 1$ and $459 \cdot 2^{8529} + 1$ are prime, see [8, p. 87]. By Lemma 8, for $x = 459 \cdot 2^{8529} + 1$ the computation $\mathcal{D}$ returns positive integers $x_1, \ldots, x_7$. Since $x > 720! = f(7)$, the statement Ψ_7 guarantees that the computation $\mathcal{D}$ returns positive integers $x_1, \ldots, x_7$ for infinitely many positive integers x. By Lemma 8, there are infinitely many twin primes. □

References

[1] C. K. Caldwell and Y. Gallot, *On the primality of $n! \pm 1$ and $2 \times 3 \times 5 \times \cdots \times p \pm 1$,* Math. Comp. 71 (2002), no. 237, 441–448.

[2] M. Erickson, A. Vazzana, D. Garth, *Introduction to number theory,* 2nd ed., CRC Press, Boca Raton, FL, 2016.

[3] W. Narkiewicz, *Rational number theory in the 20th century: From PNT to FLT,* Springer, London, 2012.

[4] W. Sierpiński, *Elementary theory of numbers,* 2nd ed. (ed. A. Schinzel), PWN – Polish Scientific Publishers and North-Holland, Warsaw-Amsterdam, 1987.

[5] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A002981, Numbers n such that $n! + 1$ is prime,* `http://oeis.org/A002981`.

[6] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A002982, Numbers n such that $n! - 1$ is prime,* `http://oeis.org/A002982`.

[7] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A093804, Primes p such that $p! + 1$ is also prime,* `http://oeis.org/A093804`.

[8] S. Y. Yan, *Number theory for computing,* 2nd ed., Springer, Berlin, 2002.

Apoloniusz Tyszka
Technical Faculty
Hugo Kołłątaj University
Balicka 116B, 30-149 Kraków, Poland
E-mail: `rttyszka@cyf-kr.edu.pl`