

A common approach to Brocard's problem, the problem of the infinitude of primes of the form  $n^2 + 1$ , and the twin prime problem

Apoloniusz Tyszka

**Abstract**

Let  $f(3) = 4$ , and let  $f(n + 1) = f(n)!$  for every integer  $n \geq 3$ . For an integer  $n \geq 3$ , let  $\Phi_n$  denote the following statement: if a system  $\mathcal{S} \subseteq \{x_i! = x_{i+1} : 1 \leq i \leq n - 1\} \cup \{x_i \cdot x_j = x_{j+1} : 1 \leq i \leq j \leq n - 1\}$  has at most finitely many solutions in integers  $x_1, \dots, x_n$  greater than 1, then each such solution  $(x_1, \dots, x_n)$  satisfies  $x_1, \dots, x_n \leq f(n)$ . We conjecture that the statements  $\Phi_3, \dots, \Phi_{16}$  are true. We prove: (1) if the equation  $x! + 1 = y^2$  has only finitely many solutions in positive integers, then the statement  $\Phi_6$  implies that each such solution  $(x, y)$  belongs to the set  $\{(4, 5), (5, 11), (7, 71)\}$ ; (2) the statement  $\Phi_9$  proves the implication: if there exists an integer  $x$  such that  $x^2 + 1$  is prime and  $x^2 + 1 > f(7)$ , then there are infinitely many primes of the form  $n^2 + 1$ ; (3) the statement  $\Phi_{16}$  proves the implication: if there exists a twin prime greater than  $f(14)$ , then there are infinitely many twin primes.

**Key words and phrases:** Brocard's problem, Brocard-Ramanujan Diophantine equation, prime numbers of the form  $n^2 + 1$ , single query to the halting oracle, twin prime conjecture.

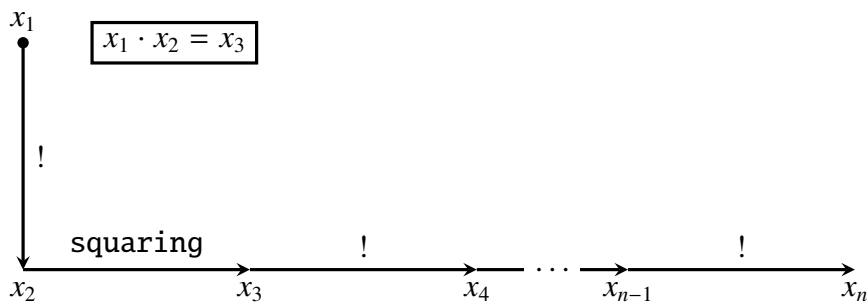
**2010 Mathematics Subject Classification:** 11A41, 11D85.

**1 Introduction and basic lemmas**

In this article, we propose a conjecture which provides a common approach to Brocard's problem, the problem of the infinitude of primes of the form  $n^2 + 1$ , and the twin prime problem. Let  $f(3) = 4$ , and let  $f(n + 1) = f(n)!$  for every integer  $n \geq 3$ . For an integer  $n \geq 3$ , let  $\mathcal{U}_n$  denote the following system of equations:

$$\begin{cases} \forall i \in \{1, \dots, n - 1\} \setminus \{2\} & x_i! = x_{i+1} \\ & x_1 \cdot x_2 = x_3 \\ & x_2 \cdot x_2 = x_3 \end{cases}$$

The diagram in Figure 1 illustrates the construction of the system  $\mathcal{U}_n$ .



**Fig. 1** Construction of the system  $\mathcal{U}_n$

**Lemma 1.** For every integer  $n \geq 3$ , the system  $\mathcal{U}_n$  has exactly one solution in integers greater than 1, namely  $(2, 2, f(3), \dots, f(n))$ .

Let

$$B_n = \{x_i! = x_{i+1} : 1 \leq i \leq n-1\} \cup \{x_i \cdot x_j = x_{j+1} : 1 \leq i \leq j \leq n-1\}$$

For an integer  $n \geq 3$ , let  $\Phi_n$  denote the following statement: if a system  $\mathcal{S} \subseteq B_n$  has at most finitely many solutions in integers  $x_1, \dots, x_n$  greater than 1, then each such solution  $(x_1, \dots, x_n)$  satisfies  $x_1, \dots, x_n \leq f(n)$ . We conjecture that the statements  $\Phi_3, \dots, \Phi_{16}$  are true. For every integer  $n \geq 3$ , the system  $B_n$  has a finite number of subsystems. Therefore, every statement  $\Phi_n$  is true with an integer bound that depends on  $n$ .

**Lemma 2.** For every statement  $\Phi_n$ , the bound  $f(n)$  cannot be decreased.

*Proof.* It follows from Lemma 1 because  $\mathcal{U}_n \subseteq B_n$ . □

**Lemma 3.** For every integers  $x$  and  $y$  greater than 1,  $x! \cdot y = y!$  if and only if  $x + 1 = y$ .

**Lemma 4.** If  $x \geq 4$ , then  $\frac{(x-1)! + 1}{x} > 1$ .

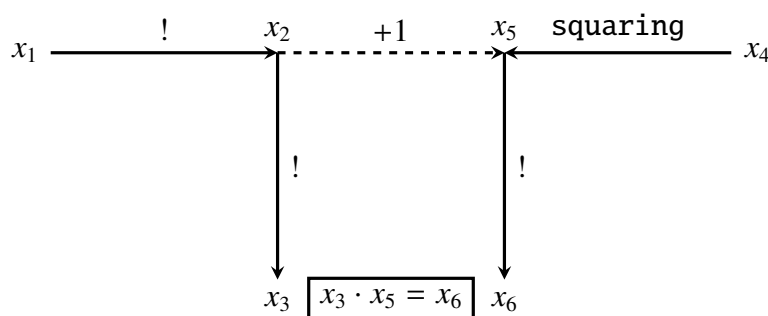
**Lemma 5.** (Wilson's theorem, [2, p. 89]) For every integer  $x \geq 2$ ,  $x$  is prime if and only if  $x$  divides  $(x-1)! + 1$ .

## 2 Brocard's problem

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

$$\begin{cases} x_1! = x_2 \\ x_2! = x_3 \\ x_5! = x_6 \\ x_4 \cdot x_4 = x_5 \\ x_3 \cdot x_5 = x_6 \end{cases}$$

Lemma 3 and the diagram in Figure 2 explain the construction of the system  $\mathcal{A}$ .



**Fig. 2** Construction of the system  $\mathcal{A}$

**Lemma 6.** For every integers  $x_1$  and  $x_4$  greater than 1, the system  $\mathcal{A}$  is solvable in integers  $x_2, x_3, x_5, x_6$  greater than 1 if and only if  $x_1! + 1 = x_4^2$ . In this case, the integers  $x_2, x_3, x_5, x_6$  are uniquely determined by the following equalities:

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

*Proof.* It follows from Lemma 3. □

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

**Theorem 1.** *If the equation  $x_1! + 1 = x_4^2$  has only finitely many solutions in positive integers, then the statement  $\Phi_6$  implies that each such solution  $(x_1, x_4)$  belongs to the set  $\{(4, 5), (5, 11), (7, 71)\}$ .*

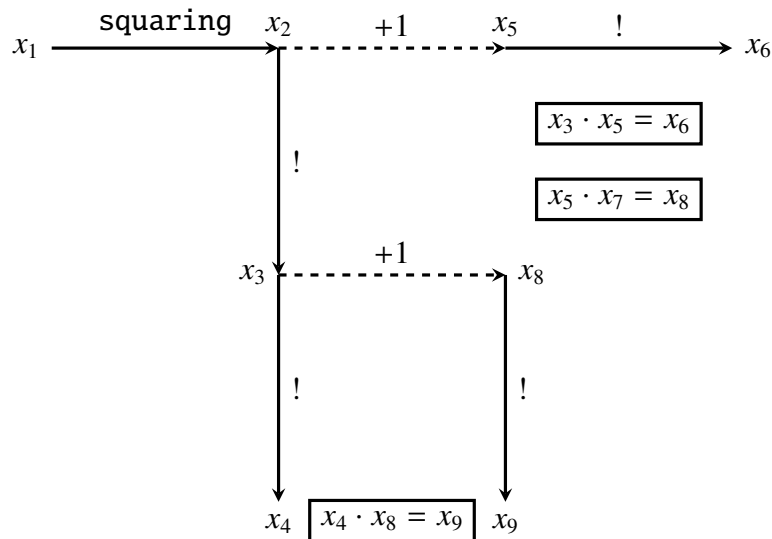
*Proof.* Assume that the antecedent holds. Assume that positive integers  $x_1$  and  $x_4$  satisfy  $x_1! + 1 = x_4^2$ . Then,  $x_1, x_4 \in \mathbb{N} \setminus \{0, 1\}$ . By Lemma 6, the system  $\mathcal{A}$  is solvable in integers  $x_2, x_3, x_5, x_6$  greater than 1. Since  $\mathcal{A} \subseteq B_6$ , the statement  $\Phi_6$  implies that  $x_6 = (x_1! + 1)! \leq f(6) = f(5)!$ . Hence,  $x_1! + 1 \leq f(5) = f(4)!$ . Consequently,  $x_1 < f(4) = 24$ . If  $x_1 \in \{2, \dots, 23\}$ , then  $x_1! + 1$  is a perfect square only for  $x_1 \in \{4, 5, 7\}$ . □

### 3 Are there infinitely many prime numbers of the form $n^2 + 1$ ?

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

$$\left\{ \begin{array}{l} x_2! = x_3 \\ x_3! = x_4 \\ x_5! = x_6 \\ x_8! = x_9 \\ x_1 \cdot x_1 = x_2 \\ x_3 \cdot x_5 = x_6 \\ x_4 \cdot x_8 = x_9 \\ x_5 \cdot x_7 = x_8 \end{array} \right.$$

Lemma 3 and the diagram in Figure 3 explain the construction of the system  $\mathcal{B}$ .



**Fig. 3** Construction of the system  $\mathcal{B}$

**Lemma 7.** *For every integer  $x_1 \geq 2$ , the system  $\mathcal{B}$  is solvable in integers  $x_2, \dots, x_9$  greater than 1 if and only if  $x_1^2 + 1$  is prime. In this case, the integers  $x_2, \dots, x_9$  are uniquely determined by the*

following equalities:

$$\begin{aligned}
x_2 &= x_1^2 \\
x_3 &= (x_1^2)! \\
x_4 &= ((x_1^2)!) \\
x_5 &= x_1^2 + 1 \\
x_6 &= (x_1^2 + 1)! \\
x_7 &= \frac{(x_1^2)! + 1}{x_1^2 + 1} \\
x_8 &= (x_1^2)! + 1 \\
x_9 &= ((x_1^2)! + 1)!
\end{aligned}$$

*Proof.* By Lemmas 3 and 4, for every integer  $x_1 \geq 2$ , the system  $\mathcal{B}$  is solvable in integers  $x_2, \dots, x_9$  greater than 1 if and only if  $x_1^2 + 1$  divides  $(x_1^2)! + 1$ . Hence, the claim of Lemma 7 follows from Lemma 5.  $\square$

Landau's conjecture states that there are infinitely many primes of the form  $n^2 + 1$ , see [3, pp. 37–38].

**Theorem 2.** *The statement  $\Phi_9$  proves the implication: if there exists an integer  $x_1$  such that  $x_1^2 + 1$  is prime and greater than  $f(7)$ , then there are infinitely many primes of the form  $n^2 + 1$ .*

*Proof.* Assume that the antecedent holds. By Lemma 7, there exists a unique tuple  $(x_2, \dots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^8$  such that the tuple  $(x_1, x_2, \dots, x_9)$  solves the system  $\mathcal{B}$ . Since  $x_1^2 + 1 > f(7)$ , we obtain that  $x_1^2 \geq f(7)$ . Hence,  $(x_1^2)! \geq f(7)! = f(8)$ . Consequently,

$$x_9 = ((x_1^2)! + 1)! \geq (f(8) + 1)! > f(8)! = f(9)$$

Since  $\mathcal{B} \subseteq B_9$ , the statement  $\Phi_9$  and the inequality  $x_9 > f(9)$  imply that the system  $\mathcal{B}$  has infinitely many solutions  $(x_1, \dots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^9$ . According to Lemma 7, there are infinitely many primes of the form  $n^2 + 1$ .  $\square$

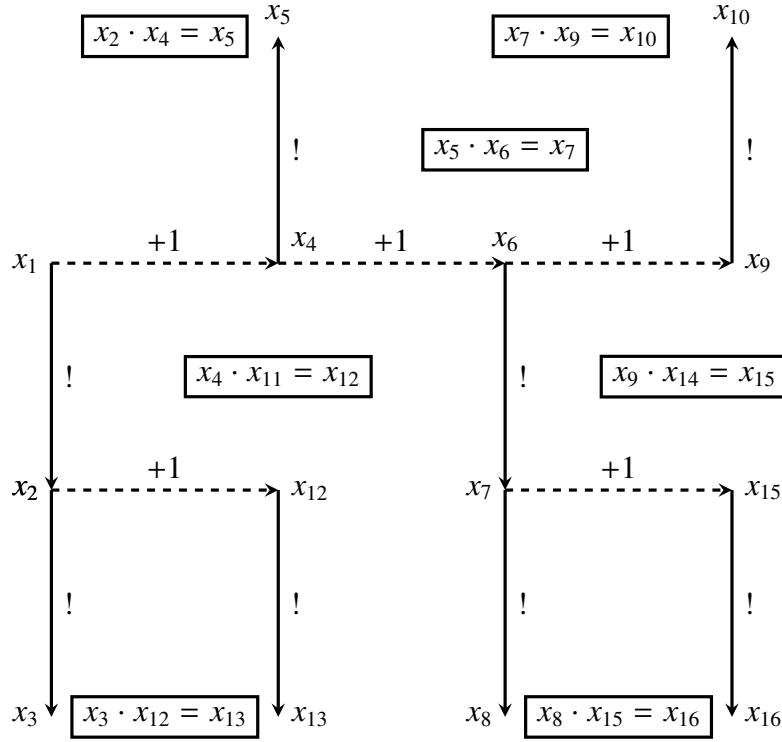
**Corollary 1.** *Assuming the statement  $\Phi_9$ , a single query to the halting oracle decides Landau's problem.*

## 4 The twin prime conjecture

Let  $C$  denote the following system of equations:

$$\left\{ \begin{array}{l}
x_1! = x_2 \\
x_2! = x_3 \\
x_4! = x_5 \\
x_6! = x_7 \\
x_7! = x_8 \\
x_9! = x_{10} \\
x_{12}! = x_{13} \\
x_{15}! = x_{16} \\
x_2 \cdot x_4 = x_5 \\
x_5 \cdot x_6 = x_7 \\
x_7 \cdot x_9 = x_{10} \\
x_4 \cdot x_{11} = x_{12} \\
x_3 \cdot x_{12} = x_{13} \\
x_9 \cdot x_{14} = x_{15} \\
x_8 \cdot x_{15} = x_{16}
\end{array} \right.$$

Lemma 3 and the diagram in Figure 4 explain the construction of the system  $C$ .



**Fig. 4** Construction of the system  $C$

**Lemma 8.** *If  $x_4 = 2$ , then the system  $C$  has no solutions in integers  $x_1, \dots, x_{16}$  greater than 1.*

*Proof.* The equality  $x_2 \cdot x_4 = x_5 = x_4!$  and the equality  $x_4 = 2$  imply that  $x_2 = 1$ .  $\square$

**Lemma 9.** *If  $x_4 = 3$ , then the system  $C$  has no solutions in integers  $x_1, \dots, x_{16}$  greater than 1.*

*Proof.* The equality  $x_4 \cdot x_{11} = x_{12} = (x_4 - 1)! + 1$  and the equality  $x_4 = 3$  imply that  $x_{11} = 1$ .  $\square$

**Lemma 10.** *For every  $x_4 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$  and for every  $x_9 \in \mathbb{N} \setminus \{0, 1\}$ , the system  $C$  is solvable in integers  $x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}$  greater than 1 if and only if  $x_4$  and  $x_9$  are prime and  $x_4 + 2 = x_9$ . In this case, the integers  $x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}$  are uniquely determined by the following equalities:*

$$\begin{aligned}
 x_1 &= x_4 - 1 \\
 x_2 &= (x_4 - 1)! \\
 x_3 &= ((x_4 - 1)!)! \\
 x_5 &= x_4! \\
 x_6 &= x_9 - 1 \\
 x_7 &= (x_9 - 1)! \\
 x_8 &= ((x_9 - 1)!)! \\
 x_{10} &= x_9! \\
 x_{11} &= \frac{(x_4 - 1)! + 1}{x_4} \\
 x_{12} &= (x_4 - 1)! + 1 \\
 x_{13} &= ((x_4 - 1)! + 1)! \\
 x_{14} &= \frac{(x_9 - 1)! + 1}{x_9} \\
 x_{15} &= (x_9 - 1)! + 1 \\
 x_{16} &= ((x_9 - 1)! + 1)!
 \end{aligned}$$

*Proof.* By Lemmas 3 and 4, for every  $x_4 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$  and for every  $x_9 \in \mathbb{N} \setminus \{0, 1\}$ , the system  $C$  is solvable in integers  $x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}$  greater than 1 if and only if

$$(x_4 + 2 = x_9) \wedge (x_4 | (x_4 - 1)! + 1) \wedge (x_9 | (x_9 - 1)! + 1)$$

Hence, the claim of Lemma 10 follows from Lemma 5. □

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 3.** *The statement  $\Phi_{16}$  proves the implication: if there exists a twin prime greater than  $f(14)$ , then there are infinitely many twin primes.*

*Proof.* Assume that the antecedent holds. Then, there exist prime numbers  $x_4$  and  $x_9$  such that  $x_9 = x_4 + 2 > f(14)$ . Hence,  $x_4 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$ . By Lemma 10, there exists a unique tuple  $(x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}) \in (\mathbb{N} \setminus \{0, 1\})^{14}$  such that the tuple  $(x_1, \dots, x_{16})$  solves the system  $C$ . Since  $x_9 > f(14)$ , we obtain that  $x_9 - 1 \geq f(14)$ . Therefore,  $(x_9 - 1)! \geq f(14)! = f(15)$ . Hence,  $(x_9 - 1)! + 1 > f(15)$ . Consequently,

$$x_{16} = ((x_9 - 1)! + 1)! > f(15)! = f(16)$$

Since  $C \subseteq B_{16}$ , the statement  $\Phi_{16}$  and the inequality  $x_{16} > f(16)$  imply that the system  $C$  has infinitely many solutions in integers  $x_1, \dots, x_{16}$  greater than 1. According to Lemmas 8–10, there are infinitely many twin primes. □

**Corollary 2.** *Assuming the statement  $\Phi_{16}$ , a single query to the halting oracle decides the twin prime problem.*

Corollary 2 conditionally solves the problem in [1].

## References

- [1] F. G. Dorais, *Can the twin prime problem be solved with a single use of a halting oracle?* July 23, 2011, <http://mathoverflow.net/questions/71050>.
- [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] M. Overholt, *The Diophantine equation  $n! + 1 = m^2$* , Bull. London Math. Soc. 25 (1993), no. 2, 104.
- [5] E. W. Weisstein, *CRC Concise Encyclopedia of Mathematics*, 2nd ed., Chapman & Hall/CRC, Boca Raton, FL, 2002.

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