doi: 10.17951/a.2022.76.1.17-23

ANNALES
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN – POLONIA

VOL. LXXVI, NO. 1, 2022 SECTIO A 17–23

LUIS H. GALLARDO

Bell numbers and Kurepa's conjecture

Abstract. We prove under a mild condition that Kurepa's conjecture holds for the set of prime numbers p such that $(\frac{p-1}{2})! = \left(\frac{2}{p}\right)$ in $\mathbb{F}_p$.

1. Introduction. Kurepa's conjecture states that for any odd prime number p, we have

$$0! + 1! + \cdots + (p-1)! \not\equiv 0 \pmod{p}. \tag{1}$$

We let $!p$ (as usual) denote the expression on the left-hand side of (1). We call it the *left factorial* of p. Kurepa's conjecture (introduced by Duro Kurepa in 1971 [17]) is a long-standing difficult conjecture. We do not know any infinite set of prime numbers for which the conjecture holds. Moreover, Barsky and Benzaghou [5, 6] failed to prove it. Details about work on the conjecture appear in [2–4, 8, 11, 14, 16, 18, 19, 21, 23–25, 27, 28, 30–33].

The purpose of the present paper is to prove the conjecture in one special case. This can be achieved with the aid of the Bell numbers. We now recall some facts about them.

Definition 1. The Bell numbers $B(n)$ are defined by $B(0) := 1$, and

$$B(n+1) := \sum_{k=0}^{n} \binom{n}{k} B(k).$$

2010 *Mathematics Subject Classification.* Primary 11T55, 11T06; Secondary 11B73, 11B65, 05A10, 12E20, 11A07, 11A25.

Key words and phrases. Artin–Schreier extension, Bell numbers, Kurepa conjecture.

The Bell numbers $B(n)$ are positive integers that arise in combinatorics. Besides the classical Definition 1 that comes from Becker and Riordan [7], other definitions, or characterizations, appear in [1], [9], [10, p. 371], [22]. To be more precise, let us fix the notation throughout the paper in Section 2.

In the following, we use the notation in Section 2.

The link of r with the Bell numbers $B(n)$ modulo p [5], [20, Theorem 8.24], is the following equality:

$$B(n) = -\mathrm{Tr}(r^{c(p)})\mathrm{Tr}(r^{n-c(p)-1}) \text{ in } \mathbb{F}_p. \tag{2}$$

Gallardo and Rahavandrainy [12] generalized the Bell number $B(n) \in \mathbb{F}_p$ to some rational fraction of r, $\beta(n) \in \mathbb{F}_q$ (see Definition 4), with the property

$$\mathrm{Tr}(\beta(n)) = -B(n). \tag{3}$$

Our contribution in the present paper is to observe an unnoticed simple fact. Motivated by some computations, we realized that there seem to be few odd primes p for which

$$\beta(p-1) = r^{c(p)} \text{ in } \mathbb{F}_q. \tag{4}$$

Nevertheless, always $\beta(p-1) = kr^{c(p)}$ for some $k \in \mathbb{F}_p$, see Lemma 6.

More precisely, it seems that the only solutions p of (4) are $p = 3$ and $p = 10331$.

Since Kurepa's conjecture for a prime number p fails if and only if (see Lemma 10)

$$B(p-1) = 1 \text{ in } \mathbb{F}_p \tag{5}$$

and equations (2) and (3) hold, we are able to easily deduce the result described in the abstract (see the short proof in Section 4).

Essentially, the idea of the proof is to look for prime numbers for which (4) and (5) are equivalent, since these primes should be counter-examples to Kurepa's conjecture.

Namely, in the present paper, we prove the following result:

Theorem 2. *Assume that the only odd prime solutions p of $\beta(p-1) = r^{c(p)}$ in $\mathbb{F}_q$, are $p = 3$ and $p = 10331$. Then $!p_1 \neq 0$ in $\mathbb{F}_{p_1}$ for all odd primes p_1 for which $(\frac{p_1-1}{2})! = \left(\frac{2}{p_1}\right)$ in $\mathbb{F}_{p_1}$.*

Remark 3.

(a) By computations in gp-PARI (that lasted about 64 hours) we know that the only odd prime numbers $p < 4000000$ for which $\beta(p-1) = r^{c(p)}$ in $\mathbb{F}_q$ are $p = 3$ and $p = 10331$.

(b) The primes p_1 such that $(\frac{p_1-1}{2})! = \left(\frac{2}{p_1}\right)$ in $\mathbb{F}_{p_1}$ appear to be (but without proof) exactly those in the OEIS sequence A129517 [29]. Of course, we do not know if the sequence contains an infinite number of entries. In other words, we do not know if our theorem holds for infinitely many prime numbers.

2. Notation. We call an integer d a *period* of $B(n) \pmod p$ if for all nonnegative integers n one has $B(n+d) \equiv B(n) \pmod p$. For each prime number p, Williams [34] proved that the sequence $B(n) \pmod p$ is periodic. We set $q := p^p$. Let $\mathbb{F}_p$ denote the finite field with p elements and $\mathbb{F}_q$ denote the finite field with q elements. Let r be a root of the irreducible trinomial $x^p - x - 1 \in \mathbb{F}_p[x]$ in some fixed algebraic closure of $\mathbb{F}_p$. The field $\mathbb{F}_q = \mathbb{F}_p(r)$ is the Artin–Schreier extension of degree p of $\mathbb{F}_p$. We denote by Tr the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$. We put $c(p) := 1 + 2p + 3p^2 + \cdots + (p-1)p^{p-2}$, and recall that $!p := 0! + 1! + \cdots + (p-1)!$. For convenience of the reader, we repeat here some definitions from [12] that we need for the proof.

Motivated by the definition of the falling and rising powers of positive integers (see, e.g., [13, pages 248–250]), we define the following:

Definition 4. Set $\epsilon(i) := (r+i+1)\cdots(r+p-1)$ in $\mathbb{F}_q$ for $i = 0, \ldots, p-2$, and $\epsilon(p-1) := 1$, $\epsilon(p) := \epsilon(0)$. More generally, we extend the definition to any integer n by putting $\epsilon(n) := \epsilon(n \pmod p)$.

Definition 5. We put for every integer n,

$$\beta(n) := \sum_{i=0}^{p-1} (r+i)^n \epsilon(i) \text{ in } \mathbb{F}_q. \tag{6}$$

3. Tools. The following lemma [12, Lemma 7] is about the $p-1$ roots of r in $\mathbb{F}_q$.

Lemma 6. *The set of $y \in \mathbb{F}_q$ such that $y^p = ry$ equals $\{kr^{c(p)} \colon k \in \mathbb{F}_p\}$.*

We also have the following result:

Lemma 7. *Let n be any nonnegative integer. With the same notation as before, we have the following:*

$$\mathrm{Tr}(\beta(n)) = -B(n) \text{ in } \mathbb{F}_p.$$

Kahale [15, formula (3)] (see also [26]), proved the following:

Lemma 8. *Let p be an odd prime number. One has*

$$B(c(p)) = (-1)^{\frac{(p-1)(p-3)}{8}} \left(\frac{p-1}{2}\right)!$$

in $\mathbb{F}_p$.

The next result is [12, Lemma 42 (a)].

Lemma 9. *We have*

$$\mathrm{Tr}(r^{c(p)}) = B(c(p)) \text{ in } \mathbb{F}_p.$$

The link between Kurepa's conjecture (1) and Bell numbers [5, p. 2] is the following statement:

Lemma 10. *Let p be an odd prime number. Then,*

$$!p = 0 \text{ in } \mathbb{F}_p \text{ if and only if } B(p-1) = 1 \text{ in } \mathbb{F}_p.$$

For completeness, we give a short proof of the next classical result.

Lemma 11. *Let p be an odd prime number. We have*

$$-1 = (p-1)! = \left(\frac{p-1}{2}\right)!^{2} \cdot (-1)^{\frac{p-1}{2}} \text{ in } \mathbb{F}_p.$$

Proof. First, observe that Wilson's theorem says that

$$-1 = (p-1)! \text{ in } \mathbb{F}_p. \tag{7}$$

Second, we compute $(p-1)!$ in $\mathbb{F}_p$ as follows:

$$(p-1)! = (1 \cdot (p-1)) \cdot (2 \cdot (p-2)) \cdots \left(\frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right)\right). \tag{8}$$

In other words, (8) implies the following equality:

$$(p-1)! = \left(\frac{p-1}{2}\right)! \cdot (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \text{ in } \mathbb{F}_p. \tag{9}$$

The result follows from (7) and (9). □

4. Proof of Theorem 2. Let p be an odd prime such that

$$\beta(p-1) = r^{c(p)} \text{ in } \mathbb{F}_q, \tag{10}$$

e.g., $p \in \{3, 10331\}$. Taking the trace Tr in both sides of (10), by Lemma 7 and Lemma 9 we obtain

$$-B(p-1) = B(c(p)) \text{ in } \mathbb{F}_p. \tag{11}$$

Now we use the explicit form of $B(c(p))$ in Lemma 8 to write (11) as

$$-B(p-1) = (-1)^{\frac{(p-1)(p-3)}{8}} \cdot \left(\frac{p-1}{2}\right)! \text{ in } \mathbb{F}_p. \tag{12}$$

Replacing (-1) in the left-hand side of (12) and using Lemma 11, we get

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \cdot (-1)^{\frac{p-1}{2}} \cdot B(p-1) = (-1)^{\frac{(p-1)(p-3)}{8}} \cdot \left(\frac{p-1}{2}\right)! \text{ in } \mathbb{F}_p. \tag{13}$$

Multiplying both sides of equation (12) by $(-1)^{\frac{p-1}{2}}$, we obtain

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \cdot B(p-1) = (-1)^{\frac{(p-1)(p-3)}{8}} \cdot (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \text{ in } \mathbb{F}_p. \tag{14}$$

But

$$(-1)^{\frac{(p-1)(p-3)}{8}} \cdot (-1)^{\frac{p-1}{2}} = (-1)^{\frac{p^2-4p+3}{8} + \frac{4p-4}{8}} = (-1)^{\frac{p^2-1}{8}}. \tag{15}$$

Thus, (14) implies that

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \cdot B(p-1) = (-1)^{\frac{(p^2-1}{8}} \cdot \left(\frac{p-1}{2}\right)! \text{ in } \mathbb{F}_p. \tag{16}$$

But $\left(\frac{p-1}{2}\right)! \neq 0$ in $\mathbb{F}_p$. Dividing both sides of (16) by $\left(\left(\frac{p-1}{2}\right)!\right)^2$, we obtain

$$B(p-1) = \frac{\left(\frac{2}{p}\right)}{\left(\frac{p-1}{2}\right)!} \text{ in } \mathbb{F}_p, \tag{17}$$

since by the quadratic law of reciprocity of Gauss, one has

$$(-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right). \tag{18}$$

Now we take a prime p_1 such that

$$\left(\frac{p_1-1}{2}\right)! = \left(\frac{2}{p_1}\right) \text{ in } \mathbb{F}_{p_1}. \tag{19}$$

By Lemma 6 we have

$$\beta(p_1-1) = k \cdot r^{c(p_1)} \tag{20}$$

for some $k \in \mathbb{F}_{p_1}$. Thus, as before, by Lemma 7, Lemma 9, Lemma 8, and Lemma 11 we obtain (after several steps, analogous to steps (10), (11), (12), (13), (14), (15), and (16)), the following analogue of (17):

$$B(p_1-1) = k \cdot \frac{\left(\frac{2}{p_1}\right)}{\left(\frac{p_1-1}{2}\right)!} = k \text{ in } \mathbb{F}_{p_1} \tag{21}$$

since (19) holds.

If $k \neq 1$, then Kurepa's conjecture holds for p_1 by Lemma 10. If $k = 1$, then by our hypothesis we have $p_1 \in \{3, 10331\}$. But we easily check that $p_1 \notin \{3, 10331\}$.

This finishes the proof of the theorem.

Acknowledgments. We thank the referee for detailed comments and suggestions.

References

[1] Aigner, M., *A characterization of the Bell numbers*, Discrete Math. **205**(1–3) (1999), 207–210.

[2] Andrejić, V., Bostan, A., Tatarevic, M., *On distinct residues of factorials*, Publ. Inst. Math. Nouv. Sér. **100**(114) (2016), 101–106.

[3] Andrejić, V., Tatarevic, M., *Searching for a counterexample to Kurepa's conjecture*, Math. Comput. **85**(302) (2016), 3061–3068.

[4] Andrejić, V., Bostan, A., Tatarevic, M., *Improved algorithms for left factorial residues*, Inf. Process. Lett. **167** (2021), Article ID 106078, 4 pp.

[5] Barsky, D., Benzaghou, B., *Nombres de Bell et somme de factorielles*, J. Théor. Nombres Bordeaux **16**(1) (2004), 1–17.
[6] Barsky, D., Benzaghou, B., *Erratum à l'article Nombres de Bell et somme de factorielles*, J. Théor. Nombres Bordeaux **23**(2) (2011), 527.
[7] Becker, H. W., Riordan, J., *The arithmetic of Bell and Stirling numbers*, Amer. J. Math. **70** (1948), 385–394.
[8] Carlitz, L., *A note on the left factorial function*, Math. Balkanica **5** (1975), 37–42.
[9] Dalton, R. E., Levine, J., *Minimum periods, modulo p, of first order Bell exponential integers*, Math. Comp. **16** (1962), 416–423.
[10] d'Ocagne, M., *Sur une classe de nombres remarquables*, Amer. J. Math. **9** (1887), 353–380.
[11] Dragović, B., *On some finite sums with factorials*, Facta Univ., Ser. Math. Inf. **14** (1999), 1–10.
[12] Gallardo, L. H., Rahavandrainy, O., *Bell numbers modulo a prime number, traces and trinomials*, Electron. J. Comb. **21**(4) (2014), Research Paper P4.49, 30 pp.
[13] Graham, R. L., Knuth, D. E., Patashnik, O., *Concrete Mathematics. A Foundation for Computer Science*, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1989.
[14] Ivić, A., Mijajlović, Ž, *On Kurepa's problems in number theory*, Publ. Inst. Math. (Beograd) (N.S.), Duro Kurepa memorial volume, **57**(71) (1995), 19–28.
[15] Kahale, N., *New modular properties of Bell numbers*, J. Combin. Theory Ser. A **58**(1) (1991), 147–152.
[16] Kohnen, W., *A remark on the left-factorial hypothesis*, Univ. Beograd. Publ. Elektrotechn. Fak. Ser. Mat. **9** (1998), 51–53.
[17] Kurepa, D., *On the left factorial function* $!n$, Math. Balkanica **1**(1) (1971), 147–153.
[18] Kurepa, D., *Right and left factorials*, in: *Conferenze tenuti in occasione del cinquantenario dell' Unione Matematica Italiana (1972)*, Boll. Un. Mat. Ital **4**(9) (1971), 171–189.
[19] Kurepa, D., *On some new left factorial propositions*, Math. Balkanica **4** (1974), 383–386.
[20] Lidl, R., Niederreiter, H., *Finite Fields, Encyclopedia of Mathematics and its applications*, Cambridge University Press (1983), Reprinted, 1987.
[21] Mijajlović,Ž., *On some formulas involving* $!n$ *and the verification of the* $!n$*-hypothesis by use of computers*, Publ. Inst. Math. (Beograd) (N.S.) **47**(61) (1990), 24–32.
[22] Montgomery, P., Nahm, S., Wagstaff, Jr., S. S., *The period of the Bell numbers modulo a prime*, Math. Comp. **79**(271) (2010), 1793–1800.
[23] Petojević, A., *On Kurepa's hypothesis for the left factorial*, Filomat **12**(1) (1998), 29–37.
[24] Petojević, A., Žižović, M., *Trees and the Kurepa hypothesis for left factorial*, Filomat **13** (1999), 31–40.
[25] Petojević, A., Žižović, M., Cvejić, S. D., *Difference equations and new equivalents of the Kurepa hypothesis*, Math. Morav. **3** (1999), 39–42.
[26] Radoux, Chr., *Déterminants de Hankel et théorème de Sylvester*, in: *Séminaire Lotharingien de Combinatoire (Saint-Nabor, 1992)*, 115–122, Publ. Inst. Rech. Math. Av., 498, Univ. Louis Pasteur, Strasbourg, 1992.
[27] Šami, Z., *On generalization of functions* $n!$ *and* $!n$, Publ. Inst. Math., Nouv. Sér. **60**(74) (1996), 5–14.
[28] Šami, Z., *A sequence* $u_{n,m}$ *and Kurepa's hypothesis on left factorial*, in: *Symposium Dedicated to the Memory of Duro Kurepa (Belgrade, 1996)*, Sci. Rev. Ser. Sci. Eng. **19–20** (1996), 125–113.

[29] Sloane, N. J. A., et al., *The On-Line Encyclopedia of Integer Sequences*, published electronically at `https://oeis.org`, 2019.

[30] Stanković, J., *Über einige Relationen zwischen Fakultäten und den linken Fakultäten*, Math. Balkanica **3** (1973), 488–495.

[31] Stanković, J., Žižović, M., *Noch einige Relationen zwischen den Fakultäten und den linken Fakultäten*, Math. Balkanica **4** (1974), 555–559.

[32] Trudgian, T., *There are no socialist primes less than* 10^9, Integers **14** (2014), Paper A63, 4 pp.

[33] Vladimirov, V. S., *Left factorials, Bernoulli numbers, and the Kurepa conjecture*, Publ. Inst. Math. (Beograd) (N.S.) **72**(86) (2002), 11–22.

[34] Williams, G. T., *Numbers generated by the function* e^{e^x-1}, Amer. Math. Monthly **52** (1945), 323–327.

Luis H. Gallardo
Univ. Brest, UMR CNRS 6205
Laboratoire de Mathématiques de Bretagne Atlantique
6, Av. Le Gorgeu, C.S. 93837, Cedex 3, F-29238 Brest
France
e-mail: `Luis.Gallardo@univ-brest.fr`

Received January 1, 2022