RAD HAZU. MATEMATIČKE ZNANOSTI
Vol. 27 = 555 (2023): 111-121
DOI: https://doi.org/10.21857/9e31lh6ovm

ARTIN-SCHREIER, ERDŐS, AND KUREPA'S CONJECTURE

Luis H. Gallardo

Abstract. We discuss possible generalizations of Erdős's problem about factorials in $\mathbb{F}_p$ to the Artin-Schreier extension $\mathbb{F}_{p^p}$ of $\mathbb{F}_p$. The generalizations are related to Bell numbers in $\mathbb{F}_p$ and to Kurepa's conjecture.

1. Introduction

Erdős [20, Section B44] asked for primes $p > 5$ for which $2!, 3!, \dots, (p-1)!$ are all distinct in $\mathbb{F}_p$, the finite field with p elements. Trudgian [37] discovered new congruences for p and proved that $p > 10^9$. More recently Andrejić and Tatarević [2] improved the result to $p > 2^{34}$ and Andejić et al. [4] to $p > 2^{40}$ as a by-product of the computations that proved that Kurepa's conjecture holds for $p \leq 2^{40}$.

Probably, a preliminary question was to find the primes p for which all factorials

$$0!, 1!, \dots, (p-1)!$$

are distinct in $\mathbb{F}_p$, but of course $0! = 1!$ eliminate this case immediately. We might think that the next case was to consider, instead, the factorials $1!, \dots, (p-1)!$, and observe that $1! = (p-2)!$ eliminate this case as well.

Let r be a zero of $x^p - x - 1$ in a fixed algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. The value of r is fixed throughout the entire paper.

Put $q = p^p$. The field $\mathbb{F}_q = \mathbb{F}_p(r)$ is the Artin-Schreier extension of degree p of $\mathbb{F}_p$.

Gallardo and Rahavandrainy [12] generalized the Stirling numbers in $\mathbb{F}_p$ to the *generalized Stirling numbers*

$$S(n,k) = (r + p - 1)^{\underline{p-1-k}}(r+k)^n \in \mathbb{F}_q$$

(see Definition 2.1). Thus, $\beta(n) = \sum_{k=0}^{p-1} S(n,k) \in \mathbb{F}_q$ (see Definition 2.2) play the role in $\mathbb{F}_q$ of the Bell number $B(n) \in \mathbb{F}_p$. More precisely (see Lemma 3.8

2020 *Mathematics Subject Classification.* 11T55, 11T06, 11B73, 11B65, 05A10, 12E20, 11A07, 11A25.

Key words and phrases. Artin-Schreier extension, Bell numbers, Erdős's problem on factorials modulo p, Kurepa's conjecture.

(c)), one has that $-B(n)$ equals the trace of $\beta(n)$. We can think that $\beta(n)$ extends the Bell number $B(n)$ in $\mathbb{F}_p$ to $\mathbb{F}_q$.

We discuss two analogous problems in $\mathbb{F}_q$. First, we replace the factorials $k!$ by $S_g(k) \in \mathbb{F}_q$ defined by

$$S_g(k) := S(-1, k)$$

in the statement of Erdős's question. Second, we replace these factorials by $\beta(n) \in \mathbb{F}_q$.

The common point of the two problems is that both are related to Kurepa's conjecture. More precisely, they are related to the values in $\mathbb{F}_p$ that take the *left factorial* function of a prime p:

$$!p = 0! + 1! + \cdots + (p-1)!. \tag{1.1}$$

The following recalls some known facts.

Definition 1.1. *The Bell numbers $B(n)$ are defined by $B(0) = 1$, and*

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

The Bell numbers $B(n)$ (see sequence A000110 of the OEIS [32]) are positive integers that arise in combinatorics:

$$1, 1, 2, 5, 15, 52, 203, 877, \ldots. \tag{1.2}$$

D'Ocagne [10, page 371] began work on Bell numbers. Becker and Riordan [7] give the first formal definition in English. Later, Aigner [1], Dalton and Levine [9], and more recently Montgomery et al. [24] do progress in the subject.

Barsky and Benzaghou [5], showed that the link of r with the Bell numbers $B(n)$ modulo p is the following equality in $\mathbb{F}_p$ (see also Lidl and Niederreiter [21, Theorem 8.24]), using the notation defined in Section 2,

$$B(n) = -\mathrm{Tr}(r^{c(p)})\mathrm{Tr}(r^{n-c(p)-1}). \tag{1.3}$$

Moreover, Kurepa [16] proposed the following conjecture (Kurepa's conjecture), using the notation in (1.1). For any odd prime number p, we have

$$!p \neq 0 \in \mathbb{F}_p. \tag{1.4}$$

The conjecture becomes a long-standing difficult conjecture (see also [2–6, 8, 11–13, 15–18, 22, 23, 25–27, 30, 31, 34, 35, 37, 38]).

The link between Bell numbers and Kurepa's conjecture (see Lemma 3.8 (d)) is the following.

$$B(p-1) = !p + 1 \in \mathbb{F}_p. \tag{1.5}$$

Left factorial numbers $!p \in \mathbb{F}_p$ appear in sequence A100612 of the OEIS [32]:

$$0, 1, 4, 6, 1, 10, 13, 9, 21, 17, 2, 5, 4, 16, 18, 13, 28, \ldots. \tag{1.6}$$

Gallardo and Rahavandrainy [12, Theorem 38] proved a more general result equivalent to Kurepa's conjecture. The result easily implies our first theorem:

THEOREM 1.2. *We have that $S_g(1), \ldots, S_g(p)$ are $\mathbb{F}_p$-linearly independent if and only if $!p \neq 0 \in \mathbb{F}_p$.*

Now consider the $\beta(n)$ in $\mathbb{F}_q$. Theorem 3.1 implies that $\beta(0) = \beta(1)$. We might think that this equality is an analogue of $0! = 1! \in \mathbb{F}_p$. Thus, we consider the case when $\beta(1), \beta(2), \ldots, \beta(p-1)$ are all distinct.

REMARK 1.3. Barsky and Benzaghou [5, Lemme 3] (see Lemma 3.4), proved that $\beta(n)$ is of the form $kr^{c(p)}$ for some $k \in \mathbb{F}_p$. Moreover, (see Lemma 3.9) Shparlinski's [33] work implies that for any $k \in \mathbb{F}_p$ we have that $kr^{c(p)}$ is of the form $\beta(n)$ for some integer n.

Our second result is the following.

THEOREM 1.4. *Assume that $\beta(1), \beta(2), \ldots, \beta(p-1)$ are all distinct. Then for some $k_0 \in \mathbb{F}_p$, and some integer $n \geq p$ one has*

- $\beta(n) = k_0 r^{c(p)}$, *and*
- $B(n) = 1 - !p \in \mathbb{F}_p$.

Moreover,

(a) *When $k_0 = 0$ we have $\beta(n) = 0$ for some $n \geq p+1$ so that $!p = 1$. This implies that $p > 2^{40}$.*

(b) *When $k_0 \neq 0$ and $n < p+3$ one has*
  (1) *$n = p$ and $!p = -1$ in $\mathbb{F}_p$, so that $p \in \{5, 7, 274453, 39541338091\}$ or $p > 2^{40}$, or*
  (2) *$n = p+1$ and $!p = -2$ in $\mathbb{F}_p$, so that $p \in \{3, 23, 67, 227, 10331\}$ or $p > 2^{40}$, or*
  (3) *$n = p+2$ and $!p = -6$ in $\mathbb{F}_p$, so that $p \in \{349, 1278568703\}$ or $p > 2^{40}$.*

(c) *If either $k_0 = 0$ or $n < p+3$, then one has $p > 2^{40}$, besides possibly for*

$$p \in \{1278568703, 39541338091\}.$$

REMARK 1.5. Andrejić and Tatarevic [2] proved that a solution p of Erdős's problem satisfies

- $(!p - 1)^2 = -1 \in \mathbb{F}_p$, and
- $p > 2^{40}$.

For the convenience of the reader we give short proofs of some of our results in [12] (see Section 3). Section 4 contains the proof of Theorem 1.2, while Section 5 contains the proof of Theorem 1.4.

2. Notation

We call an integer d a *period* of $B(n) \pmod p$ if for all nonnegative integers n one has $B(n+d) \equiv B(n) \pmod p$. Williams [39] proved that, for each prime number p, the sequence $B(n) \pmod p$ is periodic.

We let Tr denote the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$. We let N denote the norm function from $\mathbb{F}_q$ into $\mathbb{F}_p$. Likewise, we let σ denote the Frobenius from $\mathbb{F}_q$ onto $\mathbb{F}_q$. We let $\sigma^{(i)}$ denote the composition of σ with itself i times. In other words, for $a \in \mathbb{F}_q$ one has $\sigma^{(0)}(a) = a$, and for each $i > 0$, $\sigma^{(i)}(a) = \sigma(\sigma^{(i-1)}(a))$.

We put $c(p) = 1 + 2p + 3p^2 + \cdots + (p-1)p^{p-2}$.

Graham et al. [19, pages 248–250]) defined the falling and rising powers. The following definition is an extension of these definitions.

Definition 2.1. *(1) Extension of falling powers. Set*

$$(r+p-1)_{p-i-1} = (r+p-1)^{\underline{p-1-i}} = (r+i+1)\cdots(r+p-1)$$

in $\mathbb{F}_q$ *for* $i = 0, \ldots, p-2$, *and* $(r+p-1)_0 = (r+p-1)^{\underline{0}} = 1, (r+p-1)_{-1} = (r+p-1)^{\underline{-1}} = (r+p-1)_{p-1}$. *More generally, we extend the definition to any integer* n *by putting* $(r+p-1)_{p-n-1} = (r+p-1)_{p-1-(n \pmod p)}$.

(2) Extension of rising powers. Set $(r+p-1)^{(1)} = (r+p-1)^{\overline{1}} = r$,

$$(r+p-1)^{(p-i-1)} = (r+p-1)^{\overline{p-1-i}} = r(r+1)\cdots(r+i)$$

in $\mathbb{F}_q$ *for* $i = 1, \ldots, p-2$, *and* $(r+p-1)^{(p)} = (r+p-1)^{\overline{p}} = 1$. *More generally, we extend the definition to any integer* n *by putting* $(r+p-1)^{(p-n-1)} = (r+p-1)^{(p-1-(n \pmod p))}$.

Definition 2.2. *We put for every integer* n

$$\beta(n) = \sum_{i=0}^{p-1} (r+p-1)^{\underline{p-1-i}}(r+i)^n. \tag{2.1}$$

3. Tools

First, we have a formula for $\beta(n)$ that follows from [12, Lemma 13 and Corollary 19 (a)].

Theorem 3.1. *One has the following equality:*

$$\beta(n) = -\frac{r^{c(p)}}{\mathrm{Tr}\big(r^{c(p)}\big)} B(n).$$

Proof. We compute $(r+p-1)^{\underline{p-1-i}}(r+i)^n$ by using the action of the Frobenius σ on r and on $r^{-c(p)}$, and formula

$$\mathrm{N}(r) = r(r+1)\cdots(r+p-1) = 1,$$

as follows:

$$(r+p-1)^{\underline{p-1-i}}(r+i)^n = \frac{(r+i)^{n-1}}{(r+p-1)^{\overline{\overline{p-i}}}} = r^{c(p)}\sigma^{(i)}(r^{-c(p)})\sigma^{(i)}(r^{n-1})$$
$$= r^{c(p)}\sigma^{(i)}(r^{-c(p)+n-1}).$$

Hence, by definition of $\beta(n)$, we obtain the following:

$$\beta(n) = r^{c(p)}\mathrm{Tr}(r^{-c(p)+n-1}). \tag{3.1}$$

The result follows from equations (3.1) and (1.3). ∎

Remark 3.2. Clearly, equation (1.3) implies that

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

Thus, Kahale's result [14, formula (3)] (see also [29])

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

and Theorem 3.1 imply that

$$\beta(n) = r^{c(p)}\cdot\frac{(-1)^{\frac{(p+1)(p-5)}{8}}}{\left(\frac{p-1}{2}\right)!}\cdot B(n).$$

But $\left(\frac{p-1}{2}\right)!^2 \in \{-1,1\}$ in $\mathbb{F}_p$. Thus,

$$\beta(n)^2 = \pm\, r^{2c(p)}B(n)^2.$$

Corollary 3.3. *One has*

$$\beta(n) = k\cdot r^{c(p)}\cdot B(n),$$

where $k \in \mathbb{F}_p$, satisfies

$$k^2 \in \{-1,1\} \text{ in } \mathbb{F}_p.$$

Second, we have some useful results of Barsky and Benzaghou, Touchard, and Shparlinski. Barsky and Benzaghou [5, Lemme 3] proved the following result about 0 and the $p-1$ roots of r.

Lemma 3.4. *The set of $y \in \mathbb{F}_q$ such that $y^p = ry$ equals $\{kr^{c(p)} : k \in \mathbb{F}_p\}$*

Touchard (see [36]) proved the following.

Lemma 3.5. (Touchard's congruence) *Let p be an odd prime number. Then for any non-negative number n one has*

$$B(n) + B(n+1) \equiv B(n+p) \pmod{p}.$$

Shparlinski [33, Theorem 2] proved the following result.

Lemma 3.6. *For any $k \in \mathbb{F}_p$ there exist at least one integer n such that $k = B(n)$. Moreover, $n \le \frac{1}{2}\binom{2p}{p}$.*

Third, we collect some results of Gallardo and Rahavandrainy [12] useful for the proof of both theorems. More precisely, we display [12, Lemma 49] as Lemma 3.7, and [12, Lemma 40], [12, Theorem 3], [12, Theorem 14], [12, Proposition 33], [12, Theorem 15] as parts $(a), (b), (c), (d), (e)$ of Lemma 3.8.

LEMMA 3.7. *The following result holds. For any period d of $B(n)$ modulo p one has*

$$\beta(d-1) = \sum_{j=0}^{p-1} \beta(j).$$

PROOF. Since $t_p = \frac{p^p-1}{p-1}$ is a period of $B(n)$ (see [5, 28]), Theorem 3.1 implies that t_p is a period for $\beta(n)$. We extend the Bell numbers $B(n)$ to negative integers (see [5, Théorème 2]) using the equality (1.3). Hence, t_p is a period of $B(n)$ for $n \in \mathbb{Z}$. We now prove that d is also a period for $B(n)$, with $n \in \mathbb{Z}$, by replacing the period t_p by $n + kt_p \geq 0$ as follows:

$$B(n+d) = B(n+d+kt_p) = B(n+kt_p) = B(n).$$

Hence,

$$\beta(d-1) = \beta(-1) = r^{c(p)}\mathrm{Tr}(r^{-c(p)-2}), \tag{3.2}$$

and, following (3.1) one has

$$\sum_{j=0}^{p-1} \beta(j) = r^{c(p)} \sum_{j=0}^{p-1} \mathrm{Tr}(r^{-c(p)+j-1}) = r^{c(p)}\mathrm{Tr}\left(r^{-c(p)-1} \cdot \frac{1-(r+1)}{1-r}\right)$$
$$= r^{c(p)}\mathrm{Tr}\left(\frac{r^{-c(p)}}{r-1}\right).$$

But $r^{t_p} = 1$, $r^{p^p} = r$, and (see [5], [12, page 5])

$$-c(p)p = t_p - p^p - c(p). \tag{3.3}$$

Thus, the result follows from (3.3), since for $x \in \mathbb{F}_q$, we have $\mathrm{Tr}(x) = \mathrm{Tr}(\sigma(x))$. More precisely,

$$\mathrm{Tr}\left(\frac{r^{-c(p)}}{r-1}\right) = \mathrm{Tr}\left(\sigma\left(\frac{r^{-c(p)}}{r-1}\right)\right) = \mathrm{Tr}\left(\frac{r^{-c(p)p}}{r}\right) = \mathrm{Tr}\left(\frac{r^{-c(p)-1}}{r}\right)$$
$$= \mathrm{Tr}(r^{-c(p)-2}).$$

□

LEMMA 3.8. *The following results hold.*

(a) *For any period d of $B(n)$ modulo p one has*

$$\beta(d-1) = \beta(p-1) - \beta(0).$$

(b) *For any integer n one has*

$$\beta(n)^p = r\beta(n).$$

(c) *Let n be any non-negative integer. With the same notations as before, we have in $\mathbb{F}_p$:*

$$\operatorname{Tr}(\beta(n)) = -B(n).$$

(d) *One has that* $\operatorname{Tr}(\beta(d-1)) = -!p \in \mathbb{F}_p$.

(e) *For a prime number p and an integer k, there exists a non-negative integer n such that $B(n) = k \in \mathbb{F}_p$ if and only if $\beta(n) = k\beta(0) \in \mathbb{F}_q$.*

Proof. We prove (a): Clearly, we can extend Touchard's congruence (see Lemma 3.5) to $n \in \mathbb{Z}$. This implies that $B(p-1) - B(0) = B(-1)$ (see also [5, Lemme 5]). Since $\beta(d-1) = \beta(-1)$, the result follows from Theorem 3.1.

We prove (b): By (3.1) the formula is equivalent to $r^{(p-1)c(p)} = r$ that follows from (3.3).

We prove (c): From Theorem 3.1 one has

$$\operatorname{Tr}(\beta(n)) = -\frac{\operatorname{Tr}(r^{c(p)})}{\operatorname{Tr}(r^{c(p)})} B(n) = -B(n).$$

We prove (d): Follows from (3.2) and [5, Lemme 7 or Lemme 5].

Finally, we prove (e): Follows immediately from Theorem 3.1.

This proves the lemma. □

The next lemma follows from Theorem 3.1 and Lemma 3.6.

Lemma 3.9. *For any $\ell \in \mathbb{F}_p$ there exist at least one integer $n \leq \frac{1}{2}\binom{2p}{p}$ such that $\ell r^{c(p)} = \beta(n) \in \mathbb{F}_q$.*

Gallardo and Rahavandrainy [12, Theorem 38] also proved the following result. This result is key for the proof of Theorem 1.2.

Lemma 3.10. *Let n be an integer and $k \in \{1, \dots, p\}$, with p a prime number. Then the $\mathbb{F}_p$-vector space generated by the vectors $S(n,1), \dots, S(n,p) \in \mathbb{F}_q$ has dimension less than p if and only if*

$$\beta(n) = 0.$$

4. Proof of Theorem 1.2

Let d be a period of $B(n) \pmod p$. Assume that the $S_g(k)$ for $k = 1, \dots, p$ are $\mathbb{F}_p$-linearly dependent. Putting $n = d-1$ in the statement of Lemma 3.10, we obtain $\beta(d-1) = 0$. Then apply Lemma 3.8 (d) to get $!p = 0$.

If $!p = 0$ then Lemma 3.8 (c) implies that $B(d-1) = 0$. Thus, Theorem 3.1 proves that $\beta(d-1) = 0$. Hence, as before, by putting $n = d-1$ in the statement of Lemma 3.10, we obtain that the $S_g(k)$ are $\mathbb{F}_p$-linearly dependent.

Remark 4.1. Observe that it is easy to prove (using that the minimal polynomial of r has degree p) that the $S_g(k)$ are all distinct. Similarly, we can prove that the $\mathbb{F}_p$-vector space generated by them has dimension > 1.

5. Proof of Theorem 1.4

Let

$$S = \{kr^{c(p)} \colon k \in \mathbb{F}_p\}. \tag{5.1}$$

By Lemma 3.8 (b) and Lemma 3.4 we have that

$$S = \{\beta(1), \ldots, \beta(p-1), k_0 r^{c(p)}\} \tag{5.2}$$

for some $k_0 \in \mathbb{F}_p$. By Lemma 3.9

$$k_0 r^{c(p)} = \beta(n) \tag{5.3}$$

for some non-negative integer n.

Since the $\beta(j)$ are all distinct, one has that $n \geq p$.

Observe that

$$\sigma = \sum_{s \in S} s = r^{c(p)} \sum_{k \in \mathbb{F}_p, k \neq 0} k = r^{c(p)} \cdot p(p-1)/2 = 0. \tag{5.4}$$

Observe that (5.2), (5.3), and Lemma 3.7, together, implies that

$$\beta(d-1) + \beta(n) = \sigma + \beta(0) \tag{5.5}$$

for some period d, of $B(n)$ modulo p. Thus, (5.4) implies that

$$\beta(n) = \beta(0) - \beta(d-1). \tag{5.6}$$

But Lemma 3.8 (a) says that

$$\beta(p-1) = \beta(0) + \beta(d-1). \tag{5.7}$$

Adding both equations (5.5) and (5.6), we obtain

$$\beta(n) = 2\beta(0) - \beta(p-1). \tag{5.8}$$

Take the trace in both sides of (5.8). By Lemma 3.8 (c) we obtain

$$B(p-1) = 2 - B(n). \tag{5.9}$$

Lemma 3.8 (c) and Lemma 3.8 (d) implies

$$B(p-1) = !p + 1 \tag{5.10}$$

by taking the trace in both sides of (5.7). The result

$$B(n) = 1 - !p \tag{5.11}$$

follows then from (5.9) and (5.10).

Let $k_0 = 0$. Thus, $B(n) = 0$ by Theorem 3.1. Therefore, (5.11) implies that

$$!p = 1. \tag{5.12}$$

But Andrejić and Tatarević [3], and Andrejić et al. [4] proved that (5.12) implies $p > 2^{40}$. This proves (a). The proof of (b) is similar. More precisely, when $n = p$, we obtain from Lemma 3.5 that $B(p) = 2$ so that

$$!p = -1. \tag{5.13}$$

When $n = p + 1$ we get by a similar computation $B(p+1) = 3$ so that

$$!p = -2. \tag{5.14}$$

Finally, when $n = p + 2$, proceeding as before, we obtain

$$!p = -6. \tag{5.15}$$

Observe that [3,4] implies the existence of the specific primes (in the statement of (b)) for which (5.13), (5.14), and (5.15) hold, and also the inequality $p > 2^{40}$.

Part (c) follows from parts (a) and (b), and from a straightforward computation in gp-PARI, based on Lemma 3.8 (e). The computation showed that for all primes

$$p \in \{3, 5, 7, 23, 67, 227, 349, 10331, 274453\}$$

the $\beta(1), \dots, \beta(p-1)$ are *not* all distinct in $\mathbb{F}_q$. More precisely, the list of triplets $[b, a, p]$ with $1 \le a < b \le p - 1$ for which we have $\beta(a) = \beta(b)$ in $\mathbb{F}_q$ and a, b minimal, is as follows:

$$[3, 2, 3], [4, 3, 5], [4, 0, 7], [11, 0, 23], [6, 2, 67], [24, 23, 227], [16, 9, 349],$$
$$[186, 119, 10331], [659, 471, 274453].$$

For $p \in \{1278568703, 39541338091\}$ we do not know if the same result holds.

Acknowledgements.

We are indebted to the referee for useful suggestions. As a consequence, the presentation of the paper is greatly enhanced.

References

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

[2] V. Andrejić and M. Tatarević, *On distinct residues of factorials,* Publ. Inst. Math. (Beograd) (N.S.) **100** (2016), 101–106.

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

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

[5] D. Barsky and B. Benzaghou, *Nombres de Bell et somme de factorielles,* J. Théor. Nombres Bordeaux **16** (2004), 1–17.

[6] D. Barsky and B. Benzaghou, *Erratum à l'article Nombres de Bell et somme de factorielles,* J. Théor. Nombres Bordeaux **23** (2011), 527.

[7] H. W. Becker and J. Riordan, *The arithmetic of Bell and Stirling numbers,* Amer. J. Math. **70** (1948), 385–394.

[8] L. Carlitz, *A note on the left factorial function,* Math. Balkanica **5** (1975), 37–42.
[9] R. E. Dalton and J. Levine, *Minimum periods, modulo p, of first order Bell exponential integers,* Math. Comp. **16** (1962), 416–423.
[10] M. d'Ocagne, *Sur une classe de nombres remarquables*, Amer. J. Math. **9** (1887), 353–380.
[11] B. Dragović, *On some finite sums with factorials,* Facta Univ. Ser. Math. Inf. **14** (1999), 1–10.
[12] L. H. Gallardo and O. Rahavandrainy, *Bell numbers modulo a prime number, traces and trinomials,* Electron. J. Comb. **21** (2014), Research Paper P4.49, 30 pp.
[13] A. Ivić and Ž. Mijajlović, *On Kurepa's problems in number theory*, in: Đuro Kurepa memorial volume, Publ. Inst. Math. (Beograd) (N.S.), **57** (1995), 19–28.
[14] N. Kahale, *New modular properties of Bell numbers,* J. Combin. Theory Ser. A **58** (1991), 147–152.
[15] W. Kohnen, *A remark on the left-factorial hypothesis,* Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. **9** (1998), 51-53.
[16] Đ. Kurepa, *On the left factorial function* $!n$*,* Math. Balkanica **1** (1971), 147–153.
[17] Đ. R. Kurepa, *Right and left factorials*, in: Conferenze tenuti in occasione del cinquantenario dell' Unione Matematica Italiana (1972), Boll. Un. Mat. Ital (4) **9** (1974), no.suppl. fasc. 2, 171–189.
[18] Đ. Kurepa, *On some new left factorial propositions,* Math. Balkanica **4** (1974), 383–386.
[19] R. L. Graham, D. E. Knuth, and O. Patashnik, Concrete mathematics. A foundation for computer science, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1989.
[20] R. Guy, Unsolved Problems in Number Theory, Springer-Verlag, New York, 2004.
[21] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., Cambridge University Press, Cambridge, 1996.
[22] Ž. Mijajlović, *On some formulas involving* $!n$ *and the verification of the* $!n$*-hypothesis by use of computers,* Publ. Inst. Math. (Beograd) (N.S.) **47** (1990), 24–32.
[23] Ž. Mijajlović, *Fifty years of Kurepa's* $!n$ *hypothesis,* Bull. Cl. Sci. Math. Nat. Sci. Math. **46** (2021), 169–181.
[24] P. Montgomery, S. Nahm and S. S. Wagstaff, Jr., *The period of the Bell numbers modulo a prime,* Math. Comp. **79** (2010), 1793–1800.
[25] A. Petojević, *On Kurepa's hypothesis for the left factorial,* Filomat **12** (1998), 29–37.
[26] A. Petojević and M. Žižović, *Trees and the Kurepa hypothesis for left factorial,* Filomat **13** (1999), 31–40.
[27] A. Petojević, M. Žižović, and S. D. Cvejić, *Difference equations and new equivalents of the Kurepa hypothesis,* Math. Morav. **3** (1999), 39–42.
[28] C. Radoux, *Nombres de Bell, modulo p premier, et extensions de degré p de* $\mathbb{F}_p$*,* C. R. Acad. Sci. Paris Sér. A-B **281** (1975), A879–A882.
[29] C. Radoux, *Déterminants de Hankel et théorème de Sylvester*, in: Séminaire Lotharangien de Combinatoire (Saint-Nabor, 1992), Publ. Inst. Rech. Math. Av., Univ. Louis Pasteur, Strasbourg, Vol. 498, 1992, pp. 115–122.
[30] Z. Šami, *On generalization of functions* $n!$ *and* $!n$*,* Publ. Inst. Math. (Beograd) (N.S.) **60** (1996), 5–14.
[31] Z. N. Šami, *A sequence* $u_{n,m}$ *and Kurepa's hypothesis on left factorial*, in: Symposium Dedicated to the Memory of Đuro Kurepa (Belgrade, 1996), Sci. Rev. Ser. Sci. Eng., Vol. 19–20, 1996, pp. 105–113.
[32] N. J. A. Sloane et al., *The On-Line Encyclopedia of Integer Sequences*, published electronically at `https://oeis.org`, 2019.

[33] I. E. Shparlinskiy, *On the distribution of values of recurring sequences and the Bell numbers in finite fields,* European J. Combin. **12** (1991), 81–87.
[34] J. Stanković, *Über einige Relationen zwischen Fakultäten und den linken Fakultäten,* Math. Balkanica **3** (1973), 488–495.
[35] J. Stanković and M. Žižović, *Noch einige Relationen zwischen den Fakultäten und den linken Fakultäten,* Math. Balkanica **4** (1974), 555–559.
[36] J. Touchard, *Nombres exponentiels et nombres de Bernoulli,* Canad. J. Math. **8** (1956), 305–320.
[37] T. Trudgian, *There are no socialist primes less than* 10^9*,* Integers **14** (2014), Paper A63, 4 pp.
[38] V. S. Vladimirov, *Left factorials, Bernoulli numbers, and the Kurepa conjecture,* Publ. Inst. Math. (Beograd) (N.S.) **72** (2002), 11–22.
[39] G. T. Williams, *Numbers generated by the function* e^{e^x-1}*,* Amer. Math. Monthly. **52** (1945), 323–327.

Artin-Schreierova, Erdősova i Kurepina slutnja

Luis H. Gallardo

Sažetak. Raspravljamo o mogućim generalizacijama Erdősovog problema o faktorijelima u $\mathbb{F}_p$ na Artin-Schreierovo proširenje $\mathbb{F}_{p^p}$ od $\mathbb{F}_p$. Generalizacije su povezane s Bellovim brojevima u $\mathbb{F}_p$ i Kurepinom slutnjom.

Luis H. Gallardo
Univ. Brest
UMR CNRS 6205
Laboratoire de Mathématiques de Bretagne Atlantique,
F-29238 Brest
France
E-mail: Luis.Gallardo@univ-brest.fr

Received: 10.11.2022.
Revised: 26.4.2023.
Accepted: 16.5.2023.