Bell numbers modulo a prime number, traces and trinomials

Luis H. Gallardo
Mathematics
University of Brest
Brest, France
Luis.Gallardo@univ-brest.fr

Olivier Rahavandrainy
Mathematics
University of Brest
Brest, France
Olivier.Rahavandrainy@univ-brest.fr

Submitted: Jul 2, 2013; Accepted: Nov 25, 2014; Published: Dec 4, 2014
Mathematics Subject Classifications: 11T55, 11T06, 11B73, 11B65, 05A10, 12E20

Abstract

Given a prime number p, we deduce from a formula of Barsky and Benzaghou and from a result of Coulter and Henderson on trinomials over finite fields, a simple necessary and sufficient condition $\beta(n) = k\beta(0)$ in $\mathbb{F}_{p^p}$ in order to resolve the congruence $B(n) \equiv k \pmod p$, where $B(n)$ is the n-th Bell number, and k is any fixed integer. Several applications of the formula and of the condition are included, in particular we give equivalent forms of the conjecture of Kurepa that $B(p-1)$ is $\neq 1$ modulo p.

Keywords: Finite Fields; Trinomials; Artin-Schreier extension; Bell numbers; Stirling numbers; Kurepa's Conjecture

1 Introduction

Definition 1. The Bell numbers $B(n)$ are defined by $B(0) := 1$, and $B(n+1) := \sum_{k=0}^{n} \binom{n}{k} B(k)$.

The Bell numbers $B(n)$ are positive integers that arise in combinatorics. Besides the definition 1 that appears in [40], other definitions, or characterizations, exist (see, e.g. [49], [44], [17, page 371], [1]). Williams [34] proved that, for each prime number p, the sequence $B(n) \pmod p$ is periodic. In all the paper we keep the following notations. We denote by p an odd prime number. We call an integer d a *period* of $B(n) \pmod p$ if for all nonnegative integers n one has $B(n+d) \equiv B(n) \pmod p$. We set $q := p^p$; $\mathbb{F}_p$ is the finite field with p elements, and $\mathbb{F}_q$ is the finite field with q elements, the Artin-Schreier extension of degree p of $\mathbb{F}_p$ generated by an element r, a root of the irreducible trinomial $x^p - x - 1$ in some fixed algebraic closure of $\mathbb{F}_p$. We denote by Tr the trace

function from $\mathbb{F}_q$ onto $\mathbb{F}_p$, we denote by N the norm function from $\mathbb{F}_q$ onto $\mathbb{F}_p$. We put $c(p) := 1 + 2p + 3p^2 + \cdots + (p-1)p^{p-2}$.

In all the paper we use also the following definition, that is a variant of the definition in (see, e.g., [45, pages 248–250]), of the falling and rising powers.

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

The main new idea in the paper ([38], [39]) of Barsky and Benzaghou, consists of the observation that the Bell number $B(n)$ modulo p is related to the trace of a special element in $\mathbb{F}_q$ (see [38, Théorème 2]). More precisely one has

$$B(n) \equiv -Tr(r^{c(p)})\, Tr(r^{n-c(p)-1}) \pmod p. \tag{1}$$

Since $\mathrm{Tr}(r^{c(p)}) \not\equiv 0 \pmod p$ (see Lemma 8) one sees immediately by using the Additive Hilbert's Theorem 90 that $B(n) \equiv 0 \pmod p$ is equivalent to the existence of some $\lambda \in \mathbb{F}_q$ such that

$$r^{n-c(p)-1} = \lambda^p - \lambda.$$

By the change of variable $\gamma = r^{c(p)}\lambda$, we are reduced (see the details in Theorem 9) to study the trinomial equation

$$\gamma^p - r\gamma - r^n = 0$$

over $\mathbb{F}_q$. But Coulter and Henderson ([43], Lemma 10) have given an explicit condition for the solvability of the more general trinomial equation

$$x^{p^s} - ax - b = 0 \tag{2}$$

over the finite field $\mathbb{F}_{p^k}$.

Hence we can give a necessary and sufficient condition in order that $B(n) \equiv 0 \pmod p$, namely:

Theorem 3. *Let $p > 2$ be a prime number, and let n be a positive integer. Set $\beta(n) := \sum_{i=0}^{p-1}(r+i)^n\epsilon(i)$. Then $B(n) \equiv 0 \pmod p$ has a positive integer solution n if and only if $\beta(n) = 0$. Moreover $\beta(n)^p = r\beta(n)$.*

The special case $s = 1$ of (2) had already been considered, but in a less detailed form, by Segre (see [25, page 200]) and also by Svarc (see [29]).

The following lemma is a result of Touchard (see [31]).

Lemma 4 (Touchard's Congruence)**.** *Let p be an odd prime number. Then for any nonnegative number n one has*

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

The following result will be used extensively.

Lemma 5. *Let d be any period of the sequence $B(n) \pmod p$. Then $B(p-1) \equiv 1 \pmod p$ is equivalent to $B(d-1) \equiv 0 \pmod p$.*

Proof. By Touchard's congruence (see Lemma 4) one has $B(d-1)+B(d) \equiv B(d-1+p) \pmod p$, but $B(d-1+p) \equiv B(p-1) \pmod p$ and $B(d) \equiv B(0) \equiv 1 \pmod p$. Thus, $B(p-1) \equiv B(d-1)+1 \pmod p$. This proves the result. □

Moreover, it is interesting to observe that the minimal period of $B(n) \pmod p$ is conjectured, but not proved, (see [49], [42], [48], [22], [4], [44], [40]), to be equal to $g(p)$, where $g(p) := 1 + p + p^2 + \cdots + p^{p-1}$.

Now, we discuss a little some applications (see Sections 4 and 5) of the formula (1) and of Theorem 3.

Recall that a Stirling number $S(n,k)$ of the second kind (see [40]), count the number of ways to partition a set of n elements into k nonempty subsets. We will show (see Section 4) that the numbers $S_{p,r}(n,k) := (r+k)^n \epsilon(k) \in \mathbb{F}_q$, appearing as additive components of $\beta(n)$, are good $\mathbb{F}_q$ analogues of the Stirling numbers of the second kind $S(n,k)$, modulo p, since $\mathrm{Tr}(S_{p,r}(n,k))$ satisfies the same main recurrence as the $S(n,k)$ in $\mathbb{F}_p$, but with different initial conditions, (see the details in Theorem 17).

Moreover, in Theorem 38 we show an interesting relation between the dimension of the $\mathbb{F}_p$ vectorial space generated by these generalized Stirling numbers and the zeros of β in $\mathbb{F}_q$.

But, (see Theorem 14) the $\beta(n)$'s themselves, are good generalizations of the Bell numbers, modulo p, since in $\mathbb{F}_p$ one has

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

We can then characterize the n's such that $B(n) \equiv k \pmod p$ for any k (see Theorem 15) that generalizes Theorem 3.

More relations between $B(n)$ and $\beta(n)$ are shown in Section 4, including (see Theorem 24) the computation of the norm of $\beta(n)$.

Moreover, (see Section 5) we can then extend to $\mathbb{F}_q$ a formula of Sun and Zagier (see [54]) relating Bell numbers and derangement numbers. Furthermore, by combining both forms (1) and (3) of $B(n)$ several new equivalents of Kurepa's conjecture (see Theorem 28) are proposed. In particular a special case of Theorem 38 holds, (see condition (q) inTheorem 28), so that the conjecture is equivalent to the numbers $S_{p,r}(d-1,k)$ being linearly independent over $\mathbb{F}_p$ for $k = 0, \ldots, p-1$.

Finally, for completeness, (see Subsection 5.3) we explain how formula (1) simplifies some known results.

We recall that Kurepa's conjecture (see [10]) is a long-standing conjecture (see also [11, 12, 46, 9, 16, 20, 50, 28, 53, 5, 6, 32, 35, 24, 51]) that states that

$$K(p) := 0! + 1! + \cdots + (p-1)! \not\equiv 0 \pmod p \tag{4}$$

for any odd prime number p. Kurepa's conjecture may be stated with Bell numbers [38, page 2], since $K(p) = 0 \iff B(p-1) = 1$ in $\mathbb{F}_p$. We are then able (see condition (r) in

Theorem 28) to present a set of new formulae, that together are equivalent to $K(p) = 0$. One of them is

$$L(p) := \frac{1}{1 \cdot 1!} + \frac{1}{2 \cdot 2!} + \cdots + \frac{1}{(p-1) \cdot (p-1)!} \equiv 1 \pmod{p}. \tag{5}$$

1.1 Notation used in the paper

We denote by $\sigma^{-1}(x) := x^{p^{p-1}}$ the inverse of the Frobenius $\sigma(x) := x^p$ in the Galois group of $\mathbb{F}_q$ over $\mathbb{F}_p$. Observe that $\sigma(r) = r+1$ and $\sigma^{-1}(r) = r-1$. As usual, for an integer $s \geqslant 0$, $\sigma^{-1^{(s)}}(x)$ is defined by $\sigma^{-1^{(0)}}(x) := \sigma^{-1}(x)$ and for $s > 0$, $\sigma^{-1^{(s)}}(x) := \sigma^{-1}(\sigma^{-1^{(s-1)}}(x))$. The same holds also when σ^{-1} is replaced by σ.

Definition 6. We put for every integer n and every integer k

$$S_{p,r}(n,k) = \epsilon(k)(r+k)^n \tag{6}$$

and we put for every integer n

$$\beta(n) = \sum_{i=0}^{p-1} S_{p,r}(n,i). \tag{7}$$

2 Some tools

Lemma 7. *The set of solutions of the equation $y^p = ry$ in $\mathbb{F}_q$ equals $\{kr^{c(p)} \mid k \in \mathbb{F}_p\}$.*

Proof. See [38, Lemme 3]. □

Lemma 8. *Let $C := \mathrm{Tr}(y)$ where y is any nonzero solution of the equation $y^p = ry$ in $\mathbb{F}_q$. We put $A := \mathrm{Tr}(r^{c(p)})$ and $B := \mathrm{Tr}(r^{-c(p)})$. Then*

(a) A and B satisfy

$$AB \equiv -1 \pmod{p}$$

so that they are both nonzero in $\mathbb{F}_p$.

(b) C is nonzero.

Proof. The proof of (a) follows from (1) and from $1 = B(1)$. By Lemma 7 $y = \lambda r^{c(p)}$ for some $\lambda \in \mathbb{F}_p$. But y and $r^{c(p)}$ are both nonzero so that λ is nonzero. By (a) A is nonzero, the result follows then from $C = \lambda A$. □

The following theorem explains the relation between zeros of Bell numbers modulo p, and roots of some trinomials over $\mathbb{F}_p$.

Theorem 9. *Given a prime number p, there exists a positive integer n such that $B(n) \equiv 0 \pmod{p}$ if and only if the trinomial $x^p - rx - r^n$ has a root $\gamma \in \mathbb{F}_q$.*

Proof. By Lemma 8 $\mathrm{Tr}(r^{c(p)}) \neq 0$ in $\mathbb{F}_p$ so that (1) implies that the congruence is equivalent to $\mathrm{Tr}(r^{-c(p)-n}) = 0$ in $\mathbb{F}_p$. By the Additive Hilbert's Theorem 90 this is equivalent to the existence of some $\lambda \in \mathbb{F}_q$ with $r^{-c(p)-n} = \lambda^p - \lambda$. Observe that $r^{g(p)} = r(r+1)\cdots(r+p-1) = 1$. Observe also that $c(p) = \frac{p^p - g(p)}{p-1}$. Set $\gamma := r^{c(p)}\lambda$; since $c(p)(p-1) = g(p)(p-2)+1$ one sees that $r^{c(p)(p-1)} = r$ so that $r^{c(p)p} = r^{1+c(p)}$. This implies that $\lambda^p = r^{-c(p)-1}\gamma^p$. Dividing by $r^{-c(p)}$ one gets $r^{-1}\gamma^p - \gamma = r^{n-1}$. This proves the result. □

Here below the special case of [43, Theorem 3] that we need.

Lemma 10. *Let p be a prime number. Let a, b be elements of $\mathbb{F}_q$ with $a \neq 0$. Let $U(x) := x^p - ax - b \in \mathbb{F}_q[x]$. For $i = 0, \ldots, p-2$ define $s_i := \sum_{j=i}^{p-2} p^{j+1}$ and define $s_{p-1} := 0$. Let $\alpha := a^{1+p+\cdots+p^{p-1}}$ and $\beta := \sum_{i=0}^{p-1} a^{s_i} b^{p^i}$. Then the trinomial $U(x)$ has no roots in $\mathbb{F}_q$ if and only if $\alpha = 1$ and $\beta \neq 0$. Moreover $\beta^p = a\beta - b\alpha + b$.*

3 Proof of Theorem 3

By Theorem 9 it suffices to determine when the trinomial $x^p - rx - r^n$ has a root in $\mathbb{F}_q$. We apply Lemma 10 with $a = r$ and $b = r^n$. We get $\alpha = r^{g(p)} = 1$ in $\mathbb{F}_q$. This implies $\beta^p = r\beta$. We claim that $\beta = \beta(n)$. In order to compute β set $t_i := s_i + np^i$ for $i = 0, \ldots, p-2$ and set $t_{p-1} := np^{p-1}$. Since $r^{p^i} = r + i$ in $\mathbb{F}_q$ for any $i = 1, \ldots, p-1$, we get $r^{t_{p-1}} = (r+p-1)^n$; we have also $t_0 = p + \cdots + p^{p-1} + n = g(p) + n - 1$ so that $r^{t_0} = r^{n-1}$; and $t_1 = p^2 + \cdots + p^{p-1} + np = g(p) + (n-1)p - 1$ so that $r^{t_1} = \frac{(r+1)^{n-1}}{r}$. Set $\rho := r(r+1)\cdots(r+p-1)$. Since, $\rho = r^p - r = 1$, we get $r^{t_0} = r^{n-1}\rho = r^n\epsilon(0)$; analogously $r^{t_1} = r^{t_1}\rho = (r+1)^n\epsilon(1)$. If $p = 3$ we are done. Assume then that $p > 3$. Now for all $i = 2, \ldots, p-2$ we have $r^{t_i} = (r+i+1)\cdots(r+p-1)(r+i)^n = (r+i)^n\epsilon(i)$. Thus, $\beta = \beta(n)$. By Lemma 10 this proves the result since $\alpha = 1$.

4 Some applications I

First of all we need two lemmas that require some definitions.

Definition 11. Let α be an element of $\mathbb{F}_q$.

(a) We say that α has *ϵ-property* if either $\alpha = 0$ or $\alpha^{p-1} = \frac{1}{r}$.

(b) We say that α has *δ-property* if either $\alpha = 0$ or $\alpha^{p-1} = r$.

Lemma 12. *Let $S := \sum_{i=0}^{p-1} \epsilon(i)$. Let $\epsilon \in \mathbb{F}_q$ be such that ϵ has $\epsilon-$property, for example, $\epsilon = r^{-c(p)}$. Then*

$$\mathrm{Tr}(\epsilon) = \epsilon S.$$

In particular $\mathrm{Tr}(S) = -1$ so that $S \neq 0$, and $S^p = Sr$. Thus, S has $\delta-$property.

Proof. Since $\sigma(\epsilon) = \epsilon^p = \epsilon^{p-1}\epsilon = \epsilon/r$ we get $\sigma^{-1}(\epsilon) = \epsilon(r-1)$. It follows that $\sigma^{-1^{(k)}}(\epsilon) = \epsilon(r-1)(r-2)\cdots(r-k)$ for $k = 1, \ldots, p-1$. But $\mathrm{Tr}(\epsilon) = \epsilon + \sum_{k=1}^{p-1} \sigma^{-1^{(k)}}(\epsilon)$. Thus, $\mathrm{Tr}(\epsilon) = \epsilon+\epsilon(r+p-1)+\epsilon(r+p-1)(r+p-2)+\cdots+\epsilon((r+p-1)(r+p-2)\cdots(r+p-(p-1))$ $= \epsilon S$. Assume that $\epsilon \neq 0$. Since ϵ has $\epsilon-$property, Lemma 8 implies that $\mathrm{Tr}(\epsilon) \neq 0$ in $\mathbb{F}_p$. Thus, $S = \mathrm{Tr}(\epsilon)/\epsilon$ is nonzero. With $\epsilon = r^{-c(p)}$ we have $\mathrm{Tr}(S) = \mathrm{Tr}(r^{-c(p)})\mathrm{Tr}(r^{c(p)}) = -B(0) = -1$ by (1). Observe that $\epsilon S = \mathrm{Tr}(\epsilon) = \mathrm{Tr}(\epsilon)^p = \epsilon^p S^p$ so that we get $S^p = rS$. When $\epsilon = 0$ the result is obvious. □

The proof of the following lemma is omitted since it is similar (just use $\sigma(x)$ instead of $\sigma^{-1}(x)$ in the argument) to the proof of Lemma 12.

Lemma 13. *Let $T := \sum_{i=0}^{p-1} \delta(i)$. Let $\delta \in \mathbb{F}_q$ be such that δ has $\delta-$property, for example, $\delta = r^{c(p)}$. Then*

$$\mathrm{Tr}(\delta) = \delta T.$$

In particular $\mathrm{Tr}(T) = -1$ so that $T \neq 0$, and $T^p = T/r$. Thus, T has $\epsilon-$property.

Now we give some details about the $\beta(n)$ (7) defined in Theorem 3. The following theorem proves that these $\beta(n)$'s are good generalizations of the Bell numbers modulo p, to $\mathbb{F}_q$.

Theorem 14. *Let n be any nonnegative integer. With the same notations as before we have*

(a) In $\mathbb{F}_q$,

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

(b) In $\mathbb{F}_p$,

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

Proof. Set $b_n = \mathrm{Tr}(\beta(n))$. We have $\beta(0) = \sum_{i=0}^{p-1} \epsilon(i) = S$ where S is defined in Lemma 12. It follows from Lemma 12 that $\mathrm{Tr}(\beta(0)) = \mathrm{Tr}(S) = -1 = -B(0)$. Thus $b_0 = -B(0)$. Assume then that $n > 0$. We compute now $\Theta := \sum_{k=0}^{n} \binom{n}{k} \beta(k)$. We have $\Theta = \sum_{k=0}^{n} \binom{n}{k} \sum_{i=0}^{p-1} (r+i)^k \epsilon(i) = \sum_{i=0}^{p-1} \sum_{k=0}^{n} \binom{n}{k} (r+i)^k 1^{n-k} \epsilon(i) = \sum_{i=0}^{p-1} (r+i+1)^n \epsilon(i) = \sum_{i=0}^{p-1} (r+i+1)^{n+1} \epsilon(i+1)$, since $\epsilon(i) = (r+i+1)\epsilon(i+1)$. Put $j = i+1$, to get $\Theta = \sum_{j=1}^{p} (r+j)^{n+1} \epsilon(j) = \beta(n+1)$ since $\epsilon(p) = \epsilon(0)$. Thus, $\beta(n+1) = \sum_{k=0}^{n} \binom{n}{k} \beta(k)$. This proves (a). Taking the trace in both sides of (a) we get

$$b_{n+1} = \sum_{k=0}^{n} \binom{n}{k} b_k. \tag{8}$$

Set $R := -\sum_{k=0}^{n} \binom{n}{k} B(k)$. Observe that $b_0 = -B(0)$. Assume that $b_k = -B(k)$ for all $k = 1, \ldots, n$. Then from (8) it follows that $b_{n+1} = R$, but by definition (see definition 1) $R = -B(n+1)$ so that $b_{n+1} = -B(n+1)$. This proves that $b_n = -B(n)$ for all n, thereby finishing the proof of the theorem. □

We can then give a necessary and sufficient condition to solve the congruence $B(n) \equiv k$ for any integer k.

Theorem 15. *Let $p > 3$ be a prime number, and let k be an integer. Then $B(n) \equiv k \pmod{p}$ has a positive integer solution n if and only if $\beta(n) = k\beta(0)$.*

Proof. If $\beta(n) = k\beta(0)$ then it follows from Theorem 14 (b), by taking the trace, that $B(n) = k$ in $\mathbb{F}_p$. Assume now that $B(n) = k$ in $\mathbb{F}_p$. By Theorem 3 we have that $\beta(n)$ has $\delta-$property, and by Lemma 12 we have that $\beta(0)$ has $\delta-$property. By Lemma 13 we deduce that $\mathrm{Tr}(\beta(n)) = \beta(n)T$ and that $\mathrm{Tr}(\beta(0)) = \beta(0)T$. But, by Theorem 14 (b) we have also $B(n) = -\mathrm{Tr}(\beta(n))$ and $k = kB(0) = -k\mathrm{Tr}(\beta(0))$, with $T \neq 0$. Thus, the result follows from

$$\beta(n)T = k\beta(0)T. \qquad \square$$

Remark 16. We know that d is a divisor of $g(p)$ so that $d \leqslant g(p)$. We also know that $B(n)$ modulo p is periodic of minimal period d. It follows that that the least positive integer n with $B(n) \equiv k \pmod{p}$ satisfies $n \leqslant d$, so that n is bounded above by a polynomial in p, namely by $g(p)$. A big improvement of this simple upper bound is in [26], where it is proved that indeed $n < \frac{1}{2}\binom{2p}{p}$. Moreover, in [33] it is proved that $2^{2.54p} < d$. Both results are non-trivial. In other words one has

$$n < \frac{1}{2}\binom{2p}{p} < 2^{2.54p} < d.$$

Furthermore, (see [42, Lemma 1.1]) $d \equiv 1 \pmod{2p}$ and $d \equiv 1 \pmod{4p}$ when $p \equiv 3 \pmod{4}$ since d is a divisor of $g(p)$.

Now we show that the traces of the additive components of $\beta(n)$, namely the terms $\mathrm{Tr}((r+i)^n\epsilon(i))$, satisfy the same recurrence that the Stirling numbers of the second kind.

Theorem 17. *Let $p > 3$ be a prime number, and let n, k be nonnegative integers. Recall that by definition 2 $\epsilon(k) := \epsilon(k \pmod{p})$. Set $T(n,k) := \mathrm{Tr}(S_{p,r}(n,k)) = \mathrm{Tr}((r+k)^n\epsilon(k))$. Then*

$$T(n+1,k) = kT(n,k) + T(n,k-1).$$

Proof.

$$\begin{aligned}
&kT(n,k) + T(n,k-1)\\
=&k\mathrm{Tr}((r+k)^n\epsilon(k)) + \mathrm{Tr}((r+k-1)^n\epsilon(k-1))\\
=&\mathrm{Tr}(k(r+k)^n\epsilon(k)) + \mathrm{Tr}(\sigma((r+k-1)^n\epsilon(k-1)))\\
=&\mathrm{Tr}(k(r+k)^n\epsilon(k) + (r+k)^n r\epsilon(k))\\
=&\mathrm{Tr}((r+k)^{n+1}\epsilon(k)) = T(n+1,k).
\end{aligned}$$

$\square$

Remark 18. The initial conditions satisfied by the $T(n,k)$ differ from those of the Stirling numbers $S(n,k)$ of the second kind modulo p, namely one has $T(0,0) = \mathrm{Tr}(1/r) = -1$, instead of $S(0,0) = 0$. Moreover, $T(n,0) = \mathrm{Tr}(r^{n-1})$ that depends on n and it is difficult to compute for general n, while $S(n,0) = 0$; also $T(0,n) = \mathrm{Tr}(\epsilon(n)) = -1$ if $n \equiv 0 \pmod{p}$ and $T(0,n) = 0$ otherwise, while $S(0,n) = 0$ for all n.

Now we show that $B(n)$ and $\beta(n)$ differ only by a fixed nonzero element of $\mathbb{F}_q$.

Corollary 19. *(a)* $\beta(n) = -(1/T)B(n)$

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

(c) Let d be any period of the sequence $(B(n))$. Then d is also a period of the sequence $(\beta(n))$. More precisely, we have for all integers n

$$\beta(n+d) = \beta(n).$$

Proof. By Theorem 3 $\beta(n)$ has $\delta-$property so that we may apply Lemma 13 to get $\mathrm{Tr}(\beta(n)) = \beta(n)T$ and also $T \neq 0$. Now from Theorem 14 (b) we get $\mathrm{Tr}(\beta(n)) = -B(n)$. Combining both results we get (a). Since $\beta(n)$ and $r^{c(p)}$ are both solutions of the equation $y^p = ry$ in $\mathbb{F}_q$, by Lemma 7 one has $\beta(n) = cr^{c(p)}$ for some $c \in \mathbb{F}_p$. But, by Theorem 14 (b) $-B(n) = \mathrm{Tr}(\beta(n)) = c\mathrm{Tr}(r^{c(p)})$; and by (1) $B(n) = -\mathrm{Tr}(r^{c(p)})\mathrm{Tr}(r^{n-c(p)-1})$, so that $c = Tr(r^{n-c(p)-1})$. This proves (b). The latter assertion (c) follows from (a). □

This has the following non-trivial consequence:

Remark 20. We have in $\mathbb{F}_p$, for any odd prime number p and any nonnegative integer n.

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

Proof. Just apply part (a) of Corollary 19 above. The condition $T \neq 0$ is satisfied by Lemma 13. □

The corollary implies that $\beta(n)$ satisfies the same relations that $B(n)$. More precisely, (see Corollary 21 below), a) generalizes Touchard's Congruence in Lemma 4, (b) generalizes [8], Formula (6), (c) generalizes [8], Formula (5), (d) generalizes [8], Formula (4), and (e) generalizes [8], Formula (10).

See also [21]). The formulae below also follow directly from the definition of $\beta(n)$.

Corollary 21. *For all nonnegative integers n, q we have*

(a) $\beta(n+p) = \beta(n) + \beta(n+1)$,

(b) $\beta(n+p^m) = m\beta(n) + \beta(n+1)$,

(c) $\beta((n-1)p) = \beta(n)$,

(d) $\beta(n+kp) = \sum_{i=0}^{k} \binom{k}{i} \beta(n+i)$,

(e) $\beta(np^q + p^q) = q\beta(np^q) + \beta(np^{q+1})$.

In order to compute the norm of $\beta(n)$ we need

Lemma 22. *One has in* $\mathbb{F}_q$

(a) $1 = \prod_{i=0}^{p-1} \delta(i)\epsilon(i)$.

(b) $\prod_{i=0}^{p-2} \delta(i) = r^{-c(p)-1}$.

Proof. From Definition 2 every term in the product is actually equal to 1 since $\delta(i)\epsilon(i) = r^p - r = 1$. This proves (a). Observe that $r^{c(p)} = r(r+1)^2(r+2)^3 \cdots (r+p-2)^{p-1}$. Let $M = (M_{i,j})$ be the p by p matrix with with p equal lines $[r, r+1, r+2, \ldots, r+p-1]$. Namely,

$$M := \begin{bmatrix} r & r+1 & r+2 & \cdots & r+p-2 & r+p-1 \\ r & r+1 & r+2 & \cdots & r+p-2 & r+p-1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r & r+1 & r+2 & \cdots & r+p-2 & r+p-1 \\ r & r+1 & r+2 & \cdots & r+p-2 & r+p-1 \end{bmatrix}. \tag{9}$$

Consider the product π of all p^p entries of M. By (a), $\pi = 1$. On the other hand, puttting $\alpha = \prod_{i=0}^{p-2} \delta(i)$ and $\gamma = r^{c(p)}(r+p-1)^p$ one sees that α is the product of all entries in the lower triangular part of M without the last row and the last column. But, $\delta(p-1) = r(r+1)\cdots(r+p-1) = 1$ is the product of all entries in the last row of M., so α is equal to the product of all entries in the lower triangular part of M, i.e., $\alpha = \prod_{i \geqslant j} M_{i,j}$ Similarly, one sees also that γ is the product of all entries in the upper triangular part of M, i.e., $\gamma = \prod_{i \leqslant j} M_{i,j}$. Since only diagonal entries in M overlap, and the product of all diagonal entries of M is equal to $N(r) = 1$, one has

$$1 = \pi = \alpha\gamma \tag{10}$$

But the product of the elements in the last column of M equals $(r+p-1)^p = \sigma(r+p-1) = r$, so that

$$\gamma = r^{c(p)+1}.$$

Thus, from 10 it follows $\prod_{i=0}^{p-2} \delta(i) = r^{-c(p)-1}$ that proves (b). □

The following result of Kahale [8, formula (3)] is useful, (see also [23]).

Lemma 23. *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* $\mathbb{F}_p$.

Theorem 24. *Let $p > 2$ be a prime number. Let n be a nonnegative integer. Then*

(a) $N(\beta(n)) = \beta(n) r^{-c(p)}$.

(b) $N(\beta(n)) = \dfrac{(-1)^{\frac{(p+1)(p-5)}{8}}}{\left(\frac{p-1}{2}\right)!} B(n)$.

Proof. Since, by Theorem 1, $\sigma(\beta(n)) = r\beta(n)$ we have by induction $\sigma^{(k)}(\beta(n)) = r(r+1)\cdots(r+k-1)\beta(n) = \delta(k-1)\beta(n)$, so that $N(\beta(n)) = \beta(n)^p \prod_{k=0}^{p-1} \delta(k)$. But $\delta(p-1) = 1$ and $\beta(n)^p = r\beta(n)$, so by Lemma 22 (b) we get $N(\beta(n)) = \beta(n) r r^{-c(p)-1} = \beta(n) r^{-c(p)}$. This proves (a). From (a) and Corollary 19 (b) we have $N(\beta(n)) = \mathrm{Tr}(r^{n-c(p)-1})$. From (1) we deduce that $N(\beta(n)) = -B(n)/\mathrm{Tr}(r^{c(p)})$. From (1) with $n = c(p)$ we get $\mathrm{Tr}(r^{c(p)}) = B(c(p))$ since $\mathrm{Tr}(r^{-1}) = -1$. Thus $N(\beta(n)) = -\frac{B(n)}{B(c(p))}$. Observing that $-B(c(p)) = (-1)^{-1}B(c(p))$, the result (b) follows then from Lemma 23. □

5 Some applications II

5.1 Related to derangement numbers

We recall that the derangement number $D(n)$ may be defined by $D(0) = 1$ and $D(n) = nD(n-1) + (-1)^n$ for any positive integer n. An explicit formula that holds for any nonnegative integer n is

$$D(n) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \tag{11}$$

The main result of Sun and Zagier [54, Theorem 1] is that for any positive integer m not multiple of a prime number p one has in $\mathbb{F}_p$

$$(-1)^{m-1} D(m-1) = \sum_{k=1}^{p-1} \frac{B(k)}{(-m)^k}. \tag{12}$$

We will extend this formula to $\mathbb{F}_q$ in such a manner that is also valid for any m. The Δ below should play the role, in $\mathbb{F}_q$, of the derangement number, modulo p.

Definition 25. For any nonnegative integer m let

$$\Delta(m-1) := \sum_{i=0}^{p-1} \frac{\epsilon(i)}{r+i+m}.$$

Theorem 26. *For any nonnegative integer m one has*

(a) If $m = ps$, for a nonnegative integer s, we have $\Delta(m-1) = \beta(d-1)$, where d is any period of $B(n)$.

(b) $\Delta(m-1) = \sum_{k=0}^{p-1} (-m)^k \beta(p-1-k) - \beta(0)$.

(c) When $p \nmid m$ we have $\Delta(m-1) = \sum_{k=1}^{p-1} \frac{\beta(k)}{(-m)^k}$.

(d) $\mathrm{Tr}(\Delta(m-1)) = (-1)^m D(m-1)$.

(e) $1 + (-1)^{m-1} D(m-1) = \sum_{k=0}^{p-1} (-m)^k B(p-1-k)$, in $\mathbb{F}_p$.

(f) When $p \nmid m$ we recover (12), by taking traces in both sides of (c).

(g) $1+(-1)^{ps-1}D(ps-1) = B(p-1)$ *in* $\mathbb{F}_p$. *In particular we have* $1+D(p-1) = B(p-1)$.

(h) $(-1)^{m-1}D(m-1) = -\operatorname{Tr}(r^{c(p)})\operatorname{Tr}(\frac{1}{r+m}r^{-c(p)-1})$.

Proof. From Definition 25 with $m = ps$ we have

$$\Delta(m-1) = \sum_{k=0}^{p-1} \epsilon(k)(r+k)^{-1} = \beta(-1).$$

But β is periodic of period d so that it follows from Corollary 19 (c) with $n = -1$ that

$$\Delta(m-1) = \beta(d-1).$$

This proves (a). Set $\rho(m)$ the right hand side of (b). We have

$$\rho(m) = \sum_{i=0}^{p-1} \left(\sum_{k=0}^{p-1} (-1)^k m^k (r+i)^{p-1-k} \right) \epsilon(i) - \sum_{i=0}^{p-1} \epsilon(i).$$

But $(-1)^k = \binom{p-1}{k}$ in $\mathbb{F}_p$, and $(r+i+m)^{p-1} - 1 = \frac{1}{r+i+m}$. So,

$$\rho(m) = \sum_{i=0}^{p-1} ((r+i+m)^{p-1} - 1)\epsilon(i) = \Delta(m-1).$$

This proves (b). Set $\psi(m)$ the right hand side of (c). We have

$$\psi(m) = \sum_{i=0}^{p-1} \epsilon(i)(a + a^2 + \cdots + a^{p-1})$$

where $a = \frac{r+i}{-m}$. Since

$$1 + a + a^2 + \cdots + a^{p-1} = \frac{a^p - 1}{a - 1}$$

we get by using $(r+i)^p = r+i+1$ and $(-m)^p = -m$ the formula

$$\psi(m) = \sum_{i=0}^{p-1} \epsilon(i) \left(\frac{r+i+1+m}{r+i+m} - 1 \right) = \Delta(m-1).$$

This proves (c). Observe that by Theorem 14 (b) one has $\operatorname{Tr}(\beta(k)) = -B(k)$ for all $k = 1, \ldots, p-1$. Assume that $p \nmid m$. By taking the trace in both sides of (c) and by using (12) multiplied in both sides by -1, in other words, the sign $(-1)^{m-1}$ in formula (12) is transformed in a sign $(-1)^m$, we get then (d). If $p \mid m$ then by (a) we get $\Delta(m-1) = \beta(d-1)$ where d is any period of $B(n)$. From (b) we get $\Delta(m-1) = \beta(p-1) - \beta(0)$. So, proceeding as before, i.e., by taking traces, we see that (d) is equivalent

to $B(d-1) = B(p-1) - 1$. But this holds by Touchard's congruence Lemma 4 with $n = d-1$. This proves (d). In order to prove (e) take traces in both sides of (b), by using again $\mathrm{Tr}(\beta(k)) = -B(k)$ and $B(0) = 1$. This together with (d) proves (e). The same argument proves (f). Substitute $m = ps$ in both sides of (e). This proves (g). In order to prove (h), observe that by (1) one has $B(p-1-k) = -\mathrm{Tr}(r^{c(p)})\mathrm{Tr}(r^{p-1-k-c(p)-1})$. Set $\mu(m) = (-1)^{m-1}D(m-1)\mathrm{Tr}(r^{c(p)})^{-1}$. So, by (e) one has

$$\mu(m) = -\left(\sum_{k=0}^{p-1}(-1)^k m^k \mathrm{Tr}(r^{p-1-k}\cdot r^{-c(p)-1})\right)$$

but $(-1)^k = \binom{p-1}{k}$ in $\mathbb{F}_p$ so

$$\mu(m) = -\mathrm{Tr}\left(r^{-c(p)-1}\left(\sum_{k=0}^{p-1}\binom{p-1}{k}m^k r^{p-1-k} - 1\right)\right)$$

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

This proves (h). □

Corollary 27. *The minimal period of $D(m)$ modulo p is $2p$. I.e., for all m one has $D(m+2p) = D(m)$ in $\mathbb{F}_p$ and $D(m+h) = D(m)$, in $\mathbb{F}_p$, for all m implies $h \geqslant 2p$.*

Proof. By changing m by $m+p$ in Theorem 26 (h) we get

$$-D(m+p-1) = D(m-1) \tag{13}$$

in $\mathbb{F}_p$. Repeating the change we get $D(m-1+2p) = D(m-1)$. Since the minimal period h divides $2p$, it is unequal to 1 or 2 and $h \neq p$ by (13), it follows that $h = 2p$. □

5.2 Related to Kurepa's conjecture

We can retrieve the most basic relation between Bell numbers and Kurepa's conjecture as follows. All computations are in $\mathbb{F}_p$. A precise relation is $B(d-1) = K(p)$ (see Proposition 33). Moreover, from Theorem 26 (a) and (d) $D(p-1) = B(d-1)$ for any period d of $B(n)$. So $K(p) = 0 \iff D(p-1) = 0$. Alternatively, we may obtain the same result observing that $K(p) = 0 \iff B(p-1) = 1$ by Theorem 26 (g). This, together with (11), gives us the explicit equivalence (that can be checked also directly using the Bouniakowsky formula $(k-1)!(p-k)! = (-1)^k$ in $\mathbb{F}_p$).

$$\sum_{k=0}^{p-1} k! = 0 \iff \sum_{k=0}^{p-1}\frac{(-1)^k}{k!} = 0. \tag{14}$$

Observe that $K(p) = \det(G(p))$ as seen by developing by the last line the determinant where $G(p) = (g_{i,j})$ is a $(p-1) \times (p-1)$ matrix defined by $g_{1,1} = -2$, $g_{i,i} = -1$ for $i \neq 1$, $g_{i,i+1} = i+1$, $g_{i,1} = -1$ for $i \neq 1$, and $g_{i,j} = 0$ for all other i, j, namely

$$G(p) := \begin{bmatrix} -2 & 2 & 0 & \cdots & \cdots & \cdots & 0 \\ -1 & -1 & 3 & 0 & \cdots & \cdots & 0 \\ -1 & 0 & -1 & 4 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & \ddots & \ddots & \ddots & 0 \\ -1 & 0 & \cdots & \cdots & 0 & -1 & p-1 \\ -1 & 0 & \cdots & \cdots & \cdots & 0 & -1 \end{bmatrix}. \tag{15}$$

It is not difficult to see that the columns 2 to $p-1$ are $\mathbb{F}_p$-linear independent so that $rank(G(p)) \in \{p-2, p-1\}$. Thus $K(p) = 0$ is equivalent to the first column $C_1 = \sum_{j=2}^{p-1} x_j C_j$ beeing an $\mathbb{F}_p$-linear combination of the other columns. This leads to the recurrence $x_{n-1} = nx_n + 1$ in $\mathbb{F}_p$ so that

$$K(p) = 0 \iff (x_{p-1} = 1 \Longrightarrow x_2 = -1). \tag{16}$$

The few first terms are: $x_{p-1} = 1, x_{p-2} = 0, x_{p-3} = 1, x_{p-4} = -2, x_{p-5} = 9, x_{p-6} = -44, x_{p-7} = 265, x_{p-8} = -1854, x_{p-9} = 14833$; see also [20].

Another simple equivalence consists of using $B(p-1) = 1$ in $\mathbb{F}_p$, the double sum (17) that holds over the integers $\mathbb{Z}$ (see [19, formula (21)])

$$B(n) = \sum_{k=1}^{n} \sum_{i=0}^{n-k} \frac{(-1)^i k^n}{k!i!}, \tag{17}$$

and (14) to get in $\mathbb{F}_p$

$$\sum_{k=0}^{p-1} k! = 0 \iff \sum_{k=3}^{p-3} \sum_{i=0}^{p-1-k} \frac{(-1)^i}{k!i!} = 0. \tag{18}$$

Using again the fact: $K(p) = 0 \iff B(p-1) = 1$, and [52, Proposition 3.1] we get

$$\sum_{k=0}^{p-1} k! = 0 \iff \det(A(p)) = 1, \tag{19}$$

where the $(p-2) \times (p-2)$ matrix $A(p) = (a_{i,j})$ is defined by $a_{i,i} = 2$, $a_{i+1,i} = 1$, $a_{i,j} = 0$ for $i > j+1$, and $a_{i,j} = (-1)^{i+j}\binom{j-1}{i-1}$ for $j > i$, namely

$$A(p) = \begin{bmatrix} 2 & -1 & 1 & -1 & \cdots & (-1)^{p-3} \\ 1 & 2 & -\binom{2}{1} & \binom{3}{1} & \cdots & (-1)^{p-4}\binom{p-3}{1} \\ 0 & 1 & 2 & -\binom{3}{2} & \cdots & (-1)^{p-5}\binom{p-3}{2} \\ 0 & 0 & 1 & 2 & \cdots & \cdot \\ 0 & 0 & 0 & 1 & \cdots & \cdot \\ \vdots & \vdots & \vdots & \vdots & \cdots & -\binom{p-3}{p-4} \\ 0 & 0 & 0 & 0 & \cdots & 2 \end{bmatrix}$$

Below, several other equivalences.

Theorem 28. *Each of the conditions below is equivalent to the condition* $K(p) = 0$ *in* $\mathbb{F}_p$.

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

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

(c) $\mathrm{Tr}(r^{-c(p)-2}) = 0$.

(d) The vector $s \in \mathbb{F}_q$ *defined by* $s^2 = r^{-c(p)-2}$ *is an isotropic vector of the quadratic form* $Q(x) = \mathrm{Tr}(x^2)$.

(e) $B(d-2p+2) + 2B(d-2p+1) = 1$.

(f) $\mathrm{Tr}\left(r^{-c(p)-1}\frac{1}{(r+1)^2}\right) = 0$.

(g) $\mathrm{Tr}(\beta(d-1)r) = 0$.

(h) $\mathrm{Tr}\left(\frac{\epsilon}{r-1}\right) = 0 = B(2) + \cdots + B(p)$, *where* $\epsilon \in \mathbb{F}_q$ *is defined by* $r\sigma(\epsilon) = \epsilon$.

(i) $\mathrm{Tr}\left(\frac{\epsilon}{r^2}\right) = 0$ *for the same* ϵ *of (h).*

(j) $D(p-2) = 1$.

(k) $D(d-2) = 0$.

(l) $B(0) + B(1) + \cdots + B(p-1) = 0$.

(m) $\mathrm{Tr}\left(r^{-c(p)-2}\frac{r^2}{r-1}\right) = 0$.

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

(o) $B(0) + B(2) + \cdots + B(p-1) = 1$ *and* $B(1) + B(3) + \cdots + B(p-2) = -1$.

(p) $\sum_{m=0}^{p-3}(-1)^m D(m) = 0$.

(q) The vector space $V(p)$, *over* $\mathbb{F}_p$, *generated by the vectors*

$$\{S_{p,r}(d-1,k), k = 0, \cdots, p-1\}$$

has dimension less than p.

(r) In $\mathbb{F}_p$ one has $\beta_0 = \cdots = \beta_{p-2} = 0$ where

$$\beta_0 := \sum_{k=1}^{p-1} \frac{1}{k \cdot k!} - 1,$$

$$\beta_1 := \sum_{k=1}^{p-2} \frac{(-1)^k}{k \cdot (k+1)!} + 2,$$

$$\beta_2 := \sum_{k=1}^{p-3} \frac{(-1)^{k+1}}{k \cdot (k+2)!} - \frac{3}{2},$$

and for $j = 3, \ldots, p-2$

$$\beta_j := \sum_{k=0}^{p-1} A_{k,j} + s_j(k) B_{k,k} F_{k,j}, \tag{20}$$

where $F_{k,j}$ are some elements in $\mathbb{F}_p$,, $s_j(k) := -1$ when $k = j$ and $s_j(k) := 1$ otherwise; and where for $0 \leqslant j \leqslant i-1$

$$A_{i,j} := \frac{(-1)^j}{j!(i-j)!(i-j)},$$

for $j > i$ we have $A_{i,j} = 0$, and

$$A_{i,i} := (-1) \sum_{j=0}^{i-1} A_{i,j},$$

while for all i

$$B_{i,i} := \frac{(-1)^i}{i!}.$$

In order to prove the theorem, we present some useful lemmas; some of them may have an interest in their own.

First of all we recall the definition of the trace that is useful in several computations below.

Remark 29. Let K be a field that is a Galois extension of the field k with Galois group $G(K/k)$. Let $a \in K$. Then

$$\mathrm{Tr}(a) = \sum_{\sigma \in G(K/k)} \sigma(a).$$

Then we have:

(a) If the degree $d := [K : k]$ of the extension K over k, is a multiple of the characteristic $p > 0$ of k and $a \in k$ is an element of k, then since $\sigma(a) = a$ for all $\sigma \in G(K/k)$ we have:

$$\mathrm{Tr}(a) = a + a + \cdots + a = d \cdot a = 0.$$

In particular this works when $a = 1$, namely:

$$\mathrm{Tr}(1) = 0.$$

However, if the extension is the trivial extension, i.e. $K = k$ so that $G(K/k) = G(k/k) = \{id\}$ so that $d = 1$, one has instead for any $a \in k$:

(b)

$$\mathrm{Tr}(a) = id(a) = a.$$

In particular this gives for the trivial extension k/k and for $1 \in k$:

$$\mathrm{Tr}(1) = 1.$$

We will use the fields $k = \mathbb{F}_p$ and $K = \mathbb{F}_q$ where $q = p^p$ and p is an odd prime number, and the trace $\mathrm{Tr}(a)$ defined above, in all computations below.

Our first two lemmas are well known but they are key to prove the next important proposition (see Proposition 33 below) that links the generalized Bell number $\beta(d-1)$ in $\mathbb{F}_q$ with the classical left-factorial sum $K(p)$ in $\mathbb{F}_p$.

Lemma 30. *The trace* $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ *restricted to* $\mathbb{F}_p$ *is the zero function.*

Proof. Let $a \in \mathbb{F}_p \subseteq \mathbb{F}_q$. Since $\mathrm{Tr}(a) = a\mathrm{Tr}(1)$ it suffices to prove that $\mathrm{Tr}(1) = 0$. But $\mathrm{Tr}(1) = 1 + \sigma(1) + \cdots + \sigma^{(p-1)}(1) = 1 + \cdots + 1 = p \cdot 1 = 0$. Thus $\mathrm{Tr}(a) = 0$ thereby proving the lemma. □

Remark 31. However, if $tr : \mathbb{F}_p \to \mathbb{F}_p$ denotes the trace, one has $tr(1) \neq 0$ since the Galois group G of the extension field $\mathbb{F}_p$ over itself, i.e., over $\mathbb{F}_p$ is reduced to the identity function $id : x \to x$, i.e., $G = \{id\}$ so that

$$tr(1) = id(1) = 1.$$

Lemma 32. *(a) The trace of any root of the polynomial* $T_p(x) := x^p - x - 1$ *is equal to* 0. *In other words,* $\mathrm{Tr}(r) = 0$,

(b) $\mathrm{Tr}\left(\dfrac{1}{r}\right) = -1.$

Proof. Observe that $\mathrm{Tr}(r)$ is the coefficients of x^{p-1} in the polynomial $T_p(x)$. This proves (a). The minimal polynomial of $\frac{1}{r}$ is $U_p(x) = x^p + x^{p-1} - 1 = -x^p T_p(1/x)$ the reciprocal polynomial of $T_p(x)$ multiplied by -1. As before $\mathrm{Tr}(\frac{1}{r})$ is the coefficient of x^{p-1} in $U_p(x)$. This proves (b). □

Proposition 33. *We have*

$$\mathrm{Tr}(\beta(d-1)) = -K(p).$$

Proof. Observe that $v_k := \epsilon(k)(r+k)^{-1} = \frac{(r+k+1)\cdots(r+p-1)}{r+k}$ for all $k = 0, \ldots, p-1$ and that $\beta(d-1) = \sum_{k=0}^{p-1} v_k$. With the change of variable $s = r+p-k$ the trace becomes

$$\mathrm{Tr}(v_{p-k}) = \mathrm{Tr}\left(\frac{(s+1)(s+2)\cdots(s+k)}{s}\right) = -k!$$

since $\mathrm{Tr}(s^h) = \mathrm{Tr}(1) = 1$ for $h = 0$, (see Lemma 30), $\mathrm{Tr}(s^h) = 0$ for $h = 1, \ldots, p-2$, and $\mathrm{Tr}(s^{-1}) = -1$ (see Lemma 32 part (b)). □

The following lemma is a special case of [47, Corollary 2.38].

Lemma 34. *Let $v_1, \ldots, v_p \in \mathbb{F}_q$. Then $\{v_1, \ldots, v_p\}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ if and only if $\det(V) \neq 0$ where V is the following $p \times p$ matrix:*

$$V = \begin{bmatrix} v_1 & v_2 & \cdots & v_p \\ \sigma(v_1) & \sigma(v_2) & \cdots & \sigma(v_p) \\ \vdots & \vdots & & \vdots \\ \sigma^{(p-1)}(v_1) & \sigma^{(p-1)}(v_2) & \cdots & \sigma^{(p-1)}(v_p) \end{bmatrix}$$

Definition 35. The circulant matrix C with first row $c_1, \ldots, c_n$, namely

$$C = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \cdots & c_{n-1} \\ \vdots & \vdots & & \vdots \\ c_2 & c_3 & \cdots & c_1 \end{bmatrix}$$

is denoted $circ(c_1, \ldots, c_n)$.

The following is [2, Proposition 10, page A VII. 36].

Lemma 36. *Let E be a vectorial space of finite dimension n over a commutative field K. Let u be an endomorphism of E. Let $char_u(x) = \prod_{i=1}^{n}(x - \alpha_i)$ be a decomposition in linear factors over a suitable extension field of K of the characteristic polynomial of u. Let $q(x)$ be a polynomial with coefficients in K. Then*

(a) The characteristic polynomial of $q(u)$ is

$$char_{q(u)}(x) = \prod_{i=1}^{n}(x - q(\alpha_i)).$$

(b) Its trace is

$$\mathrm{Tr}(q(u)) = \sum_{i=1}^{n} q(\alpha_i).$$

(c) Its determinant is

$$det(q(u)) = \prod_{i=1}^{n} q(\alpha_i).$$

The following lemma computes the determinant of a p by p circulant C over $\mathbb{F}_q$. The formula obtained is the same that in the case of a n by n circulant with $\gcd(n,p) = 1$, but we require a special proof since C is not necessarily diagonalizable. This was first observed by Ore [18, Theorem 7], three more proofs are in Silva [27, Theorem 1], Brenner [3, Theorem 1], and Lehmer [15, Theorem 1]. For completeness we provide a short proof based in Lemma 36.

Lemma 37. *Let $v_1, \ldots, v_p \in \mathbb{F}_q$. Let $V = circ(v_1, \ldots, v_p)$. Then*

$$\det(V) = (v_1 + \cdots + v_p)^p.$$

Proof. Let $\pi = circ(0, 1, 0, \ldots, 0)$ be the p by p circulant that generates polynomially all p by p circulants. Clearly $char_\pi(x) = x^p - 1 = (x-1)^p$ is the characteristic polynomial of π. Observe that $V = R(\pi)$ where $R(x) = v_1 + v_2 x + \cdots + v_p x^{p-1}$ is the representer polynomial of V. Thus, by Lemma 36 $\det(V) = \det(R(\pi)) = R(1)^p$. But $R(1) = v_1 + \cdots + v_p$. The result follows. □

Taking now the v_i's as our generalization of the Stirling numbers modulo p we get.

Theorem 38. *Let n be an integer and $k \in \{1, \ldots, p\}$. Take $v_k := S_{p,r}(n,k)$. Then the vector space $V(p)$, over $\mathbb{F}_p$, generated by the vectors*

$$\{v_1, \ldots, v_p\}$$

has dimension less than p if and only if

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

Proof. We see that $\sigma(v_k) = r v_{k+1}$ so that $\sigma^{(s)}(v_k) = r(r+1)\cdots(r+s-1)v_{k+s}$. Applying Lemma 34 to the v_i's we get

$$V = \begin{bmatrix} v_1 & v_2 & \cdots & v_p \\ rv_2 & rv_3 & \cdots & rv_1 \\ \vdots & \vdots & & \vdots \\ r_p v_p & r_p v_1 & \cdots & r_p v_{p-1} \end{bmatrix}$$

where $r_p := r(r+1)\cdots(r+p-2)$ and the indices i of the v_i's are defined modulo p. We see that $d = \det(V)$ is up to a nonzero constant in $\mathbb{F}_p$ the same as $d_1 = \det(V_1)$ where V_1 is the left-circulant matrix

$$V_1 = \begin{bmatrix} v_1 & v_2 & \cdots & v_p \\ v_2 & v_3 & \cdots & v_1 \\ \vdots & \vdots & & \vdots \\ v_p & v_1 & \cdots & v_{p-1} \end{bmatrix}$$

But d_1 differs by ± 1 from the determinant $d_2 = \det(V_2)$ where V_2 is the circulant matrix $V_2 := circ(v_1, \ldots, v_p)$.

Using Lemma 37 we obtain

$$\det(V_2) = (v_1 + \cdots + v_p)^p = (\beta(n))^p.$$

The result follows from this. □

The following is well known.

Lemma 39. *For any period d of $B(n)$, one has*

(a) $r^d = 1$.

(b) $d \equiv 1 \pmod{2p}$.

Proof. The first assertion follows from [42, Proposition 1.2 a)]. The second assertion follows from part b) of the same proposition, precisely follows from [42, Proposition 1.2 b)], and from [42, Lemma 1.1]. □

Lemma 40. *We have*

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

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

Proof. Observe that $(r+i)^{p-1} - 1 = (r+i)^{-1}$ for all $i = 0, \ldots, p-1$. Multiplying both sides by $\epsilon(i)$ and summing over i we get $\beta(p-1) - \beta(0) = \beta(-1)$. But by Lemma 39 (a) one has

$$(r+k)^{-1} = (r+k)^{d-1}$$

for any $k = 0, \ldots, p-1$ so that

$$\beta(-1) = \sum_{k=0}^{p-1} \epsilon(k)(r+k)^{-1} = \sum_{k=0}^{p-1} \epsilon(k)(r+k)^{d-1} = \beta(d-1).$$

This proves (a). By Corollary 19 (b) we get (b). An alternative proof of (a) is as follows. By Corollary 19 (c) $\beta(d-1) = \beta(-1)$ and by Corollary 21 (a), with $n = -1$ we get $\beta(-1) = \beta(p-1) - \beta(0)$. □

We recall some known but useful properties of the trace.

Lemma 41. *For $x, y \in \mathbb{F}_q$ set*

$$\langle x, y \rangle := \mathrm{Tr}(xy),$$

and $Q(x) := \langle x, x \rangle = \mathrm{Tr}(x^2)$. Define $w_j := \frac{1}{r+j} \in \mathbb{F}_q$ for all $j = 0, \ldots, p-1$. Then

(a) $< \cdot, \cdot >: \mathbb{F}_q \to \mathbb{F}_p$ *is a $\mathbb{F}_p$-bilinear form with associate quadratic form $Q : \mathbb{F}_q \to \mathbb{F}_p$.*

(b) $\{w_0, \dots w_{p-1}\}$ *is a self-dual normal basis of* $\mathbb{F}_q$ *over* $\mathbb{F}_p$ *relative to the bilinear form* $< \cdot, \cdot >$ *. In other words, we have* $< w_i, w_j >= 0$ *if* $i \neq j$ *and* $Q(w_i) = 1$ *for all* i*. Moreover,* $w_{j+1} = \sigma(w_j)$ *for all* j*.*

In the following lemma we get the explicit values of the constants A, B of Lemma 8.

Lemma 42. *We have*

(a) $\mathrm{Tr}(r^{c(p)}) = B(c(p))$.

(b) $\mathrm{Tr}(r^{-c(p)-2}) = -\dfrac{B(d-1)}{B(c(p))}$.

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

Proof. By (1)

$$B(c(p)) = -\mathrm{Tr}(r^{c(p)})(-1). \tag{21}$$

By (1) again and by (21) $B(d-1) = -B(c(p))\mathrm{Tr}(r^{-c(p)-2})$. Since $1 = B(0)$, we get (c) from (1) and part (a). □

Lemma 43. *One has*

$$r^{-c(p)-2} = s^2, \text{ where } s = \begin{cases} r^{\frac{-c(p)-2}{2}} & \text{if } p \equiv 1 \pmod 4 \\ r^{c(p)\frac{p-1}{2}(-c(p)-2)} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. From $c(p)(p-1) = g(p)(p-2)+1$ we see that $r^{c(p)(p-1)} = r$ and that $p \equiv 1 \pmod 4$ if and only if $c(p)$ is even, so that s is well defined and satisfies the equation. □

Lemma 44. *One has*

$$(r^{-c(p)-2})^p = r^{-1-c(p)}\frac{1}{(r+1)^2}.$$

Proof. From $c(p)(p-1) = g(p)(p-2)+1$ we got $r^{-pc(p)} = r^{-1-c(p)}$ so that

$$(r^{-c(p)-2})^p = r^{-1-c(p)}(\frac{1}{r^p})^2 = r^{-1-c(p)}\frac{1}{(r+1)^2}.$$ □

Lemma 45. *Let* $x(r) \in \mathbb{F}_q$ *be such that* $x(r)^p = \frac{1}{r}x(r)$*. One has*

(a) $\mathrm{Tr}\left(\dfrac{x(r)}{r-1}\right) = x(r)\beta(d-1)$.

(b) $B(d-1) = -\mathrm{Tr}(r^{c(p)})\mathrm{Tr}\left(\dfrac{x(r)}{r-1}\right) = \displaystyle\sum_{j=2}^{p} B(j)$.

Proof. Set $a := \frac{x(r)}{r-1}$. Set $\sigma^{(0)}(a) = a$. By induction one has

$$\sigma^{(i)}(a) = \frac{1}{(r+i-1)^2}\frac{1}{r+i-2}\cdots\frac{1}{r}x(r)$$

for all $i = 0, \dots p-1$. So $\mathrm{Tr}(a) = x(r)\gamma(r)$ where

$$\gamma(r) = \frac{1}{r-1} + \frac{1}{r^2} + \frac{1}{(r+1)^2 r} + \frac{1}{(r+2)^2(r+1)r} + \cdots + \frac{1}{(r+p-2)^2(r+p-3)\cdots r}.$$

But by using the definition of $\beta(d-1)$ and the identity $r(r+1)(r+2)\cdots(r+p-1) = 1$ it is easy to check that

$$\left(\beta(d-1) - \frac{1}{r+p-1}\right) + \frac{1}{r-1} = \gamma(r)$$

i.e., that $\gamma(r) = \beta(d-1)$, so that we get (a). In order to obtain (b), we may take $x(r)$ nonzero, i.e., by using Lemma 7, we take $x(r) = r^{-c(p)}$. Observe also that by Lemma 40 (b) we have $\beta(d-1) = \mathrm{Tr}(r^{-c(p)-2})r^{c(p)}$ so that by using (a) together with (1) we get $-\mathrm{Tr}(r^{c(p)})\mathrm{Tr}\left(\frac{x(r)}{r-1}\right) = B(d-1)$. From the equalities $\frac{1}{r-1} = (r-1)^{p-1} - 1$ and $x(r) = r^{-c(p)}$ we obtain $\mathrm{Tr}\left(\frac{x(r)}{r-1}\right) = \sum_{k=1}^{p-1}\mathrm{Tr}(r^{-c(p)-1+(k+1)})$ from which, by multiplying both sides by $-\mathrm{Tr}(r^{c(p)})$ and using again (1) it follows readily the latter equality of (b). □

Lemma 46. *One has*

$$B(d-2p) = B(d-1).$$

Proof. By (1) the result is equivalent to $\mathrm{Tr}(H) = 0$, where $H = r^{-c(p)-1}(r^{d-2p} - r^{d-1})$. Using $r^p = r+1$ we see that $H = r^{-1-c(p)}\frac{1}{(r+1)^2} - r^{-c(p)-2}$. The result follows from Lemma 44. □

Lemma 47. *One has*

$$B(d-2p+2) + 2B(d-2p+1) + B(d-2p) = B(d).$$

Proof. Follows from (1) and from the identity obtained

$$r^2 + 2r + 1 = r^{2p} \tag{22}$$

by multiplying both sides of (22) by $r^{-1-c(p)-2p}$. □

Lemma 48. *(a) One has for $n \geqslant s$,*

$$\sum_{m=0}^{n} m^s \binom{n}{m} D(m) = n! \sum_{j=0}^{s} (-1)^j \binom{s}{j} n^{s-j} B(j).$$

(b) For $n = 1, \ldots, p-1$ one has

$$(-1)^n B(n) \equiv \sum_{m=1}^{p-1} (-1)^m m^n D(m-1) \pmod{p}.$$

Proof. Part (a) is the main result of [41]; part (b) is [54, Corollary 1]. □

Lemma 49. *One has*

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

More generally we have for any i not exceeding p,

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

Proof. One has $S := \sum_{j=0}^{p-1} \beta(j) = \sum_{i=0}^{p-1} \epsilon(i) \sum_{j=0}^{p-1} (r+i)^j = \sum_{i=0}^{p-1} \epsilon(i) \left(\frac{(r+i)^p - 1}{r+i-1} \right)$ so that, by using $\epsilon(i)(r+i) = \epsilon(i-1)$ and with $j = i-1$, we get

$$S = \sum_{j=-1}^{p-2} \frac{\epsilon(j)}{r+j} = \sum_{k=0}^{p-1} \frac{\epsilon(k)}{r+k} = \beta(d-1).$$

The other formula has a similar proof. □

Lemma 50. *Let p be an odd prime number. In $\mathbb{F}_p$ one has*

$$B(p) = 2.$$

Proof. Since $B(0) = 1$ and $B(1) = 1$, by Lemma 4 one has in $\mathbb{F}_p$

$$1 + 1 = B(0) + B(1) = B(0+p) = B(p).$$

This proves the result. □

Lemma 51. *One has*

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

(b) $\displaystyle\sum_{j=0}^{p-1} (-1)^j B(j) = B(p) = 2.$

Proof. Part (a) follows from Theorem 14 (b) with $n = p-1$. Part (b) follows from (a), from Theorem 14 and from Lemma 50. □

Lemma 52. *For all* $i = 0, \ldots, p-1$

$$\frac{1}{r(r+1)\cdots(r+i-1)(r+i)^2} = \frac{A_{i,0}}{r} + \frac{A_{i,1}}{r+1} + \cdots + \frac{A_{i,i-1}}{r+i-1} + \frac{A_{i,i}}{r+i} + \frac{B_{i,i}}{(r+i)^2}$$

where for $0 \leqslant j \leqslant i-1$

$$\begin{aligned} A_{i,j} :=& \frac{(-1)^j}{j!(i-j)!(i-j)} \\ A_{i,i} :=& (-1)\sum_{j=0}^{i-1} A_{i,j} \text{ and} \\ B_{i,i} :=& \frac{(-1)^i}{i!}. \end{aligned}$$

Proof. Follows from computing the partial fraction decomposition (the partial fraction decomposition procedure is described in, e.g., [13, pages 187–190]) of

$$R(x,i) := \frac{1}{x(x+1)\cdots(x+i-1)(x+i)^2}$$

and then specializing $x = r$. □

We give now more details in how $R(r,k)$ is found:

Remark 53. We write the fraction $R(x,k) = \frac{1}{x(x+1)\cdots(x+k-1)(x+k)^2}$ that when $k=0$ becomes $\frac{1}{x^2}$, in the form

$$R(x,k) = \frac{A_{i,0}}{x} + \frac{A_{i,1}}{x+1} + \cdots + \frac{A_{k,k-1}}{x+k-1} + \frac{A_{k,k}}{x+k} + \frac{B_{k,k}}{(x+k)^2} \tag{23}$$

with unknown coefficients in $\mathbb{F}_p$, and as denominators the irreducible linear divisors of the denominator $D(x)$ of $R(x,k)$ raised to powers from 1 up to the multiplicity in which they appear in $D(x)$. Next we determine the coefficient $A_{k,j} \in \mathbb{F}_p$ where $0 \leqslant j \leqslant k-1$ by computing in $\mathbb{F}_p$ as follows:

$$\begin{aligned} A_{k,j} :=& \left[R(x,k)\cdot(x+j)\right]_{x=-j} \\ =& \left[\frac{1}{x(x+1)\cdots(x+j-1)\cdot(x+j+1)\cdots(x+k-1)(x+k)^2}\right]_{x=-j} \\ =& \frac{1}{(-j)(-j+1)\cdots(-1)\cdot 1\cdots(-j+k-1)(-j+k)^2} \\ =& \frac{(-1)^j}{j!(k-j)!(k-j)}. \end{aligned}$$

The coefficients $B_{k,k}$ are determined in the same manner, namely:

$$\begin{aligned} B_{k,k} &:= \left[R(x,k)\cdot(x+k)^2\right]_{x=-k} \\ &= \left[\frac{1}{x(x+1)\cdots(x+k-1)}\right]_{x=-k} \\ &= \frac{1}{(-k)\cdot(-k+1)\cdots(-k+k-2)\cdot(-k+k-1)} \\ &= \frac{1}{(-1)^k\cdot k\cdot(k-1)\cdots(k-(k-2))\cdot(k-(k-1))} \\ &= \frac{(-1)^k}{k!}. \end{aligned}$$

In order to compute $A_{k,k}$ we multiply both sides of (23) by $(x+k)$ to get

$$\frac{1}{x(x+1)\cdots(x+k-1)(x+k)} = \sum_{j=0}^{k-1}\frac{x+k}{x+j}\cdot A_{k,j} + A_{k,k} + \frac{B_{k,k}}{x+k}. \tag{24}$$

Now we work in the $\frac{1}{t}$-adic completion $\overline{\mathbb{F}_p(t)}$ of $\mathbb{F}_p(t)$. We let x go to infinity in $\overline{\mathbb{F}_p(t)}$ in both sides of (24). This gives

$$0 = \sum_{j=0}^{k-1} A_{k,j} + A_{k,k}.$$

Finally, we observe that we can get an explicit expression for $A_{k,k}$ by using the following. Put $Q(x) = x(x+1)\cdots(x+k-1)$ so that $R(x,k) = \frac{1}{Q(x)\cdot(x+k)^2}$. We have the formula, as for the classical partial fraction decompositions over the complex numbers,

$$A_{k,k} = \left[(R(x,k)\cdot(x+k)^2)'\right]_{x=-k},$$

in which the $'$ denotes formal derivation relative to x, that becomes

$$A_{k,k} = (-1)\cdot\frac{Q'(-k)}{Q(-k)^2}$$

since $x=-k$ is a double root of the denominator of $R(x,k)$. Here $Q'(x)$ is the formal derivative of $Q(x)$ relative to x. After a short computation we obtain $Q(-k)^2 = k!^2$ and $Q'(-k) = \sum_{j=0}^{k-1}\frac{(-1)^{k-1}\cdot k!}{k-j}$ so that we obtain the explicit formula.

$$A_{k,k} = \frac{(-1)^k}{k!}\cdot\sum_{j=0}^{k-1}\frac{1}{k-j}.$$

Lemma 54. *Let $w_0 := \epsilon(0)$, $w_1 := F(w_0), \ldots, w_{p-1} := F^{(p-1)}(w_0)$. Then $\{w_i \mid i = 0,\ldots,p-1\}$ is a self-dual normal basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ relative to the bilinear form*

$$\langle x, y\rangle = \mathrm{Tr}(xy).$$

Proof. We see immediately that $w_i = \frac{\epsilon(i)}{\epsilon(i-1)} = \frac{1}{r+i}$. The result follows then from Lemma 41. □

Lemma 55. *For all $i = 0, \ldots, p-1$ one has*

$$\frac{1}{(r+i)^2} = -\frac{1}{r+i} + \frac{1}{1}\frac{1}{(r+i+1)} + \frac{1}{2}\frac{1}{(r+i+2)} + \cdots + \frac{1}{p-1}\frac{1}{(r+i+p-1)}.$$

Proof. Write $\frac{1}{(r+i)^2}$ in the $\mathbb{F}_p$–basis $\{\frac{1}{(r+j)}, j = 0, \ldots, p-1\}$. By Lemma 54 it suffices to prove that $\mathrm{Tr}(\frac{1}{r^2}\frac{1}{r+j}) = \frac{1}{j}$ when $j \neq 0$ and that $\mathrm{Tr}(\frac{1}{r^2}\frac{1}{r}) = -1$. Since $r(r+1)\cdots(r+p-1) = 1$ we can write

$$\frac{1}{r^2}\frac{1}{r+j} = \frac{(r+1)\cdots(r+j-1)(r+j+1)\cdots(r+p-1)}{r}$$

when $j \neq 0$. Thus, $\mathrm{Tr}(\frac{1}{r^2}\frac{1}{r+j}) = \frac{(p-1)!}{j}\mathrm{Tr}(\frac{1}{r}) = \frac{1}{j}$. When $j = 0$ it is better to use the identity $\frac{1}{r^2} + \frac{1}{r^3} = r^{p-3}$ to conclude that $\mathrm{Tr}(\frac{1}{r^3}) = -1$. □

Proof of Theorem 28: In what follows when we say that we get a condition, e.g., (a), this means that we prove that the condition (a) is equivalent to the condition $K(p) = 0$.

Proof. Assume that $\beta(d-1) = 0$. From Proposition 33 we get $K(p) = 0$. Now assume that $K(p) = 0$. From Proposition 33 we get $\mathrm{Tr}(\beta(d-1) = 0$. It follows from Theorem 14 (b) that $B(d-1) = 0$. Now we use Corollary 19, part (a) to deduce that $\beta(d-1) = 0$. This depends on proving $T \neq 0$. This is guaranteed by Lemma 13. Thus, we get (a). See also Remark 20. From Lemma 40 and from (a) we get (b). From Theorem 14 (b), Lemma 42 (b) and (a) we get (c) since $B(d-1) = -\mathrm{Tr}(\beta(d-1))$. From (c) and Lemma 43 we get (d). From Lemma 47, from Lemma 46 and from (a) we get that the left hand side equals $B(d) = B(0) = 1$; this proves (e). From Lemma 44 and (c) follows (f). If $\beta(d-1) = 0$ then $\mathrm{Tr}(\beta((d-1)r) = 0$. For the other direction we argue as follows. Since by Theorem 3 $r\beta(d-1) = \sigma(\beta(d-1))$ the result (g) now follows by taking traces and by using (a). From Lemma 7 we can take $\epsilon = r^{-c(p)}$. It follows then from Lemma 42 (b) that $\mathrm{Tr}\left(\frac{\epsilon}{r^2}\right) = \mathrm{Tr}\left(\frac{\epsilon}{r-1}\right) = \beta(d-1)\epsilon$ since $\sigma\left(\frac{\epsilon}{r-1}\right) = \frac{\epsilon}{r^2}$. The equality $\mathrm{Tr}\left(\frac{\epsilon}{r-1}\right) = \beta(d-1)\epsilon$ follows also from Lemma 45 (a) with $x(r) = r^{-c(p)}$. Thus, (h) and (i) follows from Lemma 45 (b). (X): One has $B(p-1) = 1$ from (b) and Corollary 19 (a). (Y): We have $D(p-1) = 0$ from (X) and Theorem 26 (g). (Z): We obtain $D(p-2) = 1$ from (Y) and (11). Thus, we get (j). Since by Lemma 39 $d - 1 = 0$ in $\mathbb{F}_p$, we get (k) by Theorem 26 (h) with $m = d-1$, and from (c), since $(r+d-1)^{-1} = (r+pk+1-1)^{-1} = r^{-1}$ for some $k \in \mathbb{Z}$. From Lemma 49, Theorem 14 and (a) it follows (l). From (h) with $\epsilon = r^{-c(p)}$ it follows (m) since $r^{-c(p)-2} \cdot r^2 = r^{-c(p)}$. While (n) follows from (m) and from Lemma 42, parts (c) and (b), together with (a) by using $\frac{r^2}{r-1} = r + 1 + \frac{1}{r-1}$. More precisely, (n) is obtained by taking traces in both sides of this equality. From Lemma 51 (b) we got $2 = B(p) = \sum_{j=0}^{p-1}(-1)^j B(j)$ that combined with (l) proves (o). From Lemma 48 (b) with $n = p-1$ and using (j) we get (p). More precisely, the Lemma gives $B(p-1) = \sum_{m=1}^{p-1}(-1)^m D(m-1)$ since $m^{p-1} = 1$ for all m in this range. Multiply both sides of this

equality by (-1), put $h = m-1$ as new variable and observe that $(-1)\cdot(-1)^{h+1} = (-1)^h$ to get $-B(p-1) = \sum_{h=0}^{p-2}(-1)^h D(h) = -D(p-2)+\sum_{h=0}^{p-3}(-1)^h D(h)$. But by (j), $D(p-2) = 1$ and by taking traces in (b) and by using Theorem 14 part (b), we obtain also $B(p-1) = 1$. This proves (p).

Alternatively we can also get (p) by taking $s = p-1$ and $n = p-1$ in Lemma 48 (a). This gives in the left hand side $\sum_{m=1}^{p-1}(-1)^m D(m)$ since $0^{p-1} = 0$, $m^{p-1} = 1$ and $\binom{p-1}{m} = (-1)^m$. But, $D(p-2) = 1$ by (j) and $D(p-1) = B(p-1) - 1$ by Theorem 26 part (g), so that $D(p-1) = 0$ since $B(p-1) = 1$ as above in the first proof of (p). Thus the left hand side becomes $\sum_{m=1}^{p-3}(-1)^m D(m) + (-1)$.

The same procedure gives in the right hand side $(-1)\cdot\sum_{j=0}^{p-1}(-1)^j(-1)^{p-1-j}B(j) = (-1)\cdot\sum_{j=0}^{p-1}B(j)$ since $(p-1)! = -1$, $\binom{p-1}{j} = (-1)^j$ and $(-1)^{p-1} = 1$. But by using Lemma 51 part (b), we obtain that the right hand side is equal to -2. Comparing both sides we get $\sum_{m=1}^{p-3}(-1)^m D(m) + (-1) = -2$ so that $\sum_{m=0}^{p-3}(-1)^m D(m) = 1 + (-1) = 0$ since $(-1)^0 \cdot D(0) = 1$. This completes the second proof of (p).

We get (q) by using Theorem 38 with $n = d-1$ and from (a). Observe that $\beta(d-1) = \sum_{k=0}^{p-1} R(r,k)$ with the notations in the proof of Lemma 52 since $r(r+1)\cdots(r+p-1) = 1$. We get the values of $A_{i,j}$, $A_{i,i}$ and $B_{i,i}$ from Lemma 52. By using Lemma 55 we have then for an appropriate $\beta_{p-1} \in \mathbb{F}_p$

$$\beta(d-1) = \frac{\beta_0}{r} + \frac{\beta_1}{r+1} + \cdots + \frac{\beta_{p-2}}{r+p-2} + \frac{\beta_{p-1}}{r+p-1} \tag{25}$$

Thus (see Lemma 54) $\beta(d-1) = 0$ is equivalent to $\beta_j = 0$ for all $j = 0, \ldots, p-1$. But $\beta(d-1) = 0$ is also equivalent to $\beta_{p-1} = 0$ since from (25) and Lemma 54 $\beta_{p-1} = \mathrm{Tr}(\frac{\beta(d-1)}{r-1}) = \mathrm{Tr}(\frac{\beta(d-1)^p}{r}) = \mathrm{Tr}(\beta(d-1)) = -B(d-1)$. This proves (r). See details in how $R(r,k)$ is found in Remark 53 just after Lemma 52. □

The conjecture has been worked out numerically (see, e.g.,[16], [37]). The latest available result (see [30]) is that it holds true for all odd prime numbers less than 10^9. This is a non trivial computation since a straightforward GP-Pari computation took 7 minutes in a relatively recent computer to get the single value $K(10^9+7) = 571737251$. Using machine idle time on our local computer we obtained (using [30]) that the conjecture is true when $2 < p \leqslant 10^9 + 785617$. However, we are not aware of the existence of any *infinite* subset of the odd prime numbers for which the conjecture holds. Set $K(n) := 0!+1!+\cdots+(n-1)!$. One of the equivalent forms of the conjecture is that for all $n \geqslant 3$ one has $n \nmid K(n)$. It is easy to check that if for some $n \geqslant 3$ one has $n \nmid K(n)$ then $kn \nmid K(kn)$ for all positive integers k (see also [10, Corollary 1.3.1]. So this form of the conjecture holds for an infinity of $n's$. Another equivalent form of the conjecture (see [10]) is that for all $n > 1$ one has $\gcd(K(n), n!) = 2$. One can check that if this condition holds for an infinity of n's then it holds for all n's since $\gcd(K(n), n!) = 2 \iff$ for all odd primes $p \leqslant n$ one has $p \nmid K(p)$. By mistake, probably confounding these two forms of the conjecture, [46] state that Kurepa proved in [10] that for an infinity of n's we have $\gcd(K(n), n) = 2$.

Recently Bencherif and Oesterlé (see [39]) discovered that the published proof of the conjecture (see [38]) had a fatal gap. In a letter to Guy (see [7, B44]) Reg. Bond proposed

(unpublished) a proof. Živcović (see [36, page 403]) says that he informed him that he later discovered an error in the proof.

Finally, we discuss other applications of formula (1).

5.3 A short summary of previous results on string of consecutive zeros of $B(n)$ in $\mathbb{F}_p$, simplified by (1)

Consider the maximal number m of consecutive zeros of $B(n)$ in $\mathbb{F}_p$. By Lemma (4) $m \leqslant p-1$. Radoux proved [21], assuming that the minimal period d of $B(n)$ satisfies $d = g(p)$, that there exists one and only one string of $p-1$ consecutive zeros by period. This was extended by Layman [14] to any period d of $B(n)$ modulo p. The exact location of the string of zeros was only given modulo $g(p)$. More precisely, let b denote the exact beginning of the string of $p-1$ consecutive zeros. Radoux give $b(p-1) \equiv p \pmod{g(p)}$, Layman give $b \equiv 1 - \frac{p^p-p}{(p-1)^2} \pmod{g(p)}$, for the location of the first zero in the string. Later Kahale [8] give $b = c(p) + 1$. We just observe here that Kahale's result follows immediately from formula (1). Indeed, since for all $k = 0, \ldots, p-2$ one has in $\mathbb{F}_p$

$$\mathrm{Tr}(r^k) = 0, \tag{26}$$

(see Lemma 32), i.e.,

$$\mathrm{Tr}(r^{c(p)+k+1-(c(p)+1)}) = 0, \tag{27}$$

so that by (1) we get immediately

$$B(c(p) + k + 1) \equiv 0 \pmod{p} \tag{28}$$

for all these k's.

Acknowledgements

We are indebted to the kind French mathematician that carefully read an old draft of this paper and suggested several improvements. We are also grateful to the referee who read in great detail a first version of the paper and gives us many interesting suggestions. The presentation of the present paper has been greatly improved by their comments.

References

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

[2] N. Bourbaki. *Éléments de Mathématique. Algèbre, Chapitres 4 à 7.* Paris etc,: Masson, VII, 422 p., 1981.

[3] J. L. Brenner. $g-$circulant matrices over a field of prime characteristic. *Illinois J. Math.*, 7:174–179, 1963.

[4] L. Carlitz. Congruences for generalized Bell and Stirling numbers. *Duke Math. J.*, 22:193–205, 1955.

[5] L. Carlitz. A note on the left factorial function. *Math. Balkanica*, 5:37–42, 1975.

[6] B. Dragović. On some finite sums with factorials. *Facta Univ., Ser. Math. Inf.*, 14:1–10, 1999.

[7] R. K. Guy. *Unsolved problems in number theory.* 2nd ed., Problem Books in Mathematics, Springer-Verlag, New York. Unsolved Problems in Intuitive Mathematics, I., 1994.

[8] N. Kahale. New modular properties of Bell numbers. *J. Combin. Theory Ser. A*, 58(1):147–152, 1991.

[9] W. Kohnen. A remark on the left-factorial hypothesis. *Univ. Beograd. Publ. Elektrotechn. Fak. Ser. Mat.*, 9:51-53, 1998.

[10] D. Kurepa. On the left factorial function $!n$. *Math. Balkanica*, 1(1):147–153, 1971.

[11] D. R. Kurepa. Right and left factorials. Conferenze tenuti in occasione del cinquantenario dell' Unione Matematica Italiana (1972), *Boll. Un. Mat. Ital*, 4(9):171–189, 1971.

[12] D. Kurepa. On some new left factorial propositions. *Math. Balkanica*, 4:383–386, 1974.

[13] S. Lang. *Algebra.* Revised third ed., Graduate Texts in Mathematics, 211, Springer-Verlag, New York, 2002.

[14] J. W. Layman. Maximum zero strings of Bell numbers modulo primes. *J. Combin. Theory Ser. A*, 40(1):161–168, 1985.

[15] D. H. Lehmer. Some properties of circulants. *J. Number Theory*, 5:43–54, 1973.

[16] 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(61):24–32, 1990.

[17] M. d'Ocagne. Sur une classe de nombres remarquables. *Amer. J. Math.*, 9:353–380, 1887.

[18] O. Ore. Some studies on cyclic determinants. *Duke Math. J.*, 18:343–354, 1951.

[19] J. Pitman. Some probabilistic aspects of set partitions. *Amer. Math. Monthly*, 104(3):201–209, 1997.

[20] A. Petojević. On Kurepa's hypothesis for the left factorial. *Filomat*, 12(1):29–37, 1998.

[21] C. Radoux. Nombres de Bell, modulo p premier, et extensions de degré p de F_p. *C. R. Acad. Sci. Paris Sér. A-B*, 281(21):A879–A882, 1975.

[22] Chr. Radoux. Arithmétique des nombres de Bell et analyse modulo p-adique. *Bull. Soc. Math. Belg.*, 29(1):13–28, 1977.

[23] Chr. Radoux. Déterminants de Hankel et théorème de Sylvester. Séminaire Lotharingien de Combinatoire (Saint-Nabor, 1992), 115–122, *Publ. Inst. Rech. Math. Av., 498, Univ. Louis Pasteur, Strasbourg,*, 1992.

[24] Z. Sǎmi. On generalization of functions $n!$ and $!n$. *Publ. Inst. Math., Nouv. Sér.*, 60(74):5–14, 1996.

[25] B. Segre. Arithmetische Eigenschaften von Galois-Räumen, I.. *Math. Ann.*, 154:195–256, 1964.

[26] I. E. Shparlinskiy. On the distribution of Values of Recurring Sequences and the Bell Numbers in Finite Fields. *Europ. J. Combinatorics*, 12:81–87, 1991.

[27] J. A. Silva. A theorem on cyclic matrices. *Duke Math. J.*, 18:821–825, 1951.

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

[29] Š. Švarc. On a class of polynomials over a finite field. *Math.-Fyz. Časopis. Slovensk. Akad. Vied.*, 10:68–80, 1960.

[30] M. Tatarevic. Searching for a counterexample to the Kurepa's left factorial hypothesis ($p < 10^9$). http://mtatar.wordpress.com/2011/07/30/kurepa/, 2011.

[31] J. Touchard. Nombres exponentiels et nombres de Bernoulli. *Canad. J. Math.*, 8:305–320, 1956.

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

[33] J. F. Voloch. On some subgroups of the multiplicative group of finite rings. *J. Théor. Nombres Bordeaux*, 16(1):233–239, 2004.

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

[35] Š. Zoran N.. A sequence $u_{n,m}$ and Kurepa's hypothesis on left factorial. Symposium Dedicated to the Memory of Duro Kurepa (Belgrade, 1996), *Sci. Rev. Ser. Sci. Eng.*, 19–20:125–113, 1996.

[36] M. Živković. The number of primes $\sum_{i=1}^{n}(-1)^{n-i}i!$ is finite. *Math. Comp.*, 68(225):403–409, 1999.

[37] M. Živković. Massive computation as a problem solving tool. *Proceedings of the 10th congress of Yugoslav mathematicians, Belgrade, Yugoslavia, January 21-24, 2001, Belgrade: University of Belgrade, Faculty of Mathematics,* pages 113–128. 2001.

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

[39] D. Barsky, Benzaghou. Erratum à l'article Nombres de Bell et somme de factorielles. *J. Théor. Nombres Bordeaux*, 23(2):527, 2011.

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

[41] R. J. Clarke, M. Sved. Derangements and Bell numbers. *Math. Mag.*, 66(5):299–303, 1993.

[42] M. Car, L. H. Gallardo, O. Rahavandrainy, L. N. Vaserstein. About the period of Bell numbers modulo a prime. *Bull. Korean Math. Soc.*, 45(1):143–155, 2008.

[43] R. Coulter, M. Henderson. A note on the roots of trinomials over a finite field. *Bull. Austral. Math. Soc.*, 69(3):429–432, 2004.

[44] R. E. Dalton, J. Levine. Minimum periods, modulo p, of first order Bell exponential integers. *Math. Comp.*, 16:416–423, 1962.

[45] R. L. Graham, D. E. Knuth, O. Patashnik. *Concrete mathematics, A foundation for computer science.* Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1989.

[46] A. Ivić, Ž. Mijajlović. On Kurepa's problems in number theory. *Publ. Inst. Math. (Beograd) (N.S.), Duro Kurepa memorial volume*, 57(71):19–28, 1995.

[47] R. Lidl, H. Niederreiter. *Finite Fields, Encyclopedia of Mathematics and its applications*. Cambridge University Press (1983), Reprinted, 1987.

[48] W. F. Lunnon, P. A. B. Pleasants, N. M. Stephens. Arithmetic properties of Bell numbers to a composite modulus I.. *Acta Arith.*, 35(1):1–16, 1979.

[49] P. Montgomery, S. Nahm, S. S. Wagstaff, Jr.. The period of the Bell numbers modulo a prime. *Math. Comp.*, 79(271):1793–1800, 2010.

[50] A. Petojević, M. Žižović. Trees and the Kurepa hypothesis for left factorial. *Filomat*, 13:31–40, 1999.

[51] A. Petojević, M. Žižović, S. D. Cvejić. Difference equations and new equivalents of the Kurepa hypothesis. *Math. Morav.*, 3:39–42, 1999.

[52] P. K. Saikia, D. Subedi. Bell numbers, determinants and series. *Proc. Indian Acad. Sci. (Math. Sci.)*, 123(2):151–166, 2013.

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

[54] Z. W. Sun, D. Zagier. On a curious property of Bell numbers. *Bull. Aust. Math. Soc.*, 84(1):153–158, 2011.