Applied Mathematics E-Notes, 23(2023), 40-48 ©
Available free at mirror sites of http://www.math.nthu.edu.tw/∼amen/
ISSN 1607-2510

Bell Numbers Modulo p^*

Luis Henri Gallardo†

Received 20 January 2022

Abstract

We prove in a few new cases (under mild conditions) that the order of $x^p - x - 1 \in \mathbb{F}_p[x]$ equals $\frac{p^p-1}{p-1}$.

1 Introduction

We are interested in a link between roots of some irreducible trinomials modulo p and some numbers that appear naturally in combinatorics. The trinomials are *primitive* when every nonzero element of the extension field $\mathbb{F}_p(r)$ of the finite field $\mathbb{F}_p$ with p elements, is a power of r, with r a zero of the trinomial. This is useful for applications like coding messages. In our case, the trinomial is $T_a(x) = x^p - x - a$, with p an odd prime, and a a generator of the group of nonzero elements of $\mathbb{F}_p$. We know that $T_a(x)$ is primitive if and only if $T(x) = T_1(x) = x^p - x - 1$ has order $g(p) = \frac{p^p-1}{p-1}$. The minimal period (see below for details) of a sequence of numbers associated to the trinomial, namely, the Bell numbers, (see below) equals $g(p)$ if and only if $T(x)$ has order $g(p)$. This conjecture, that is, the statement that for any prime number p, $T_a(x)$ is always primitive, is a long-standing difficult conjecture. Thus, it is interesting to try to get some progress on it. On the other side, the Bell numbers grows exponentially. Therefore, it is easier to work with them modulo p. The Bell numbers $B(n)$ (see sequence A000110 of the OEIS [12]) are positive integers that arise in combinatorics:

$$1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437, \dots. \tag{1}$$

For small values of p, say $p \in \{2, 3\}$, we can look directly in the link above. For example, if $p = 2$, we have that the trinomial $T(x) = x^2 - x - 1 \in \mathbb{F}_2[x]$ has effectively order $g(2) = 3$, since its roots r in $\mathbb{F}_4 = \mathbb{F}_2(r)$ have order 3. Hence, we have

$$r^3 = r \cdot r^2 = r(r + 1) = r^2 + r = r + 1 + r = 1 \in \mathbb{F}_4.$$

On the other hand, the Bell numbers modulo 2

$$1, 1, 0, 1, 1, 0, 1, 1, 0, \dots$$

have minimal period $g(2) = 3$. The computation is similar for $p = 3$.

Definition 1 *The Bell numbers $B(n)$ are defined by $B(0) = 1$, and $B(n + 1) = \sum_{k=0}^{n} \binom{n}{k} B(k)$ for $n = 0, 1, 2, \cdots$.*

Besides the classical Definition 1 that comes from Becker and Riordan [4], other definitions, or characterizations, appear in [1], [6], [7, page 371], [9]. Williams [14] proved that, for each prime number p the sequence $B(n) \pmod p$ is periodic. We are interested in its minimal period. To be more precise, let us fix the following notation for the entire paper. We let p denote an odd prime number. We call an integer d a *period* of $B(n) \pmod p$ if for all non-negative integers n one has $B(n + d) \equiv B(n) \pmod p$. We set $q = p^p$, and we let $\mathbb{F}_p$ denote the finite field with p elements, and let $\mathbb{F}_q$ denote the finite field with q elements.

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

†Univ. Brest, UMR CNRS 6205, Laboratoire de Mathématiques de Bretagne Atlantique, F-29238 Brest, France

Namely, 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 let Tr denote the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$. Observe that the Frobenius $\sigma\colon \mathbb{F}_q \mapsto \mathbb{F}_q$, such that $\sigma(t) = t^p$, transforms r into $r+1$, and in general $r+n$ into $r+n+1$ for any $n \in \mathbb{F}_p$. This will be used several times in the paper without further explanation. We put $c(p) = 1 + 2p + 3p^2 + \cdots + (p-1)p^{p-2}$ and $g(p) = 1 + p + p^2 + \cdots p^{p-1}$.

Radoux [11] conjectured that the order, $d = \mathrm{o}_p(r)$, of r in $\mathbb{F}_q^*$ equals $g(p)$. It turns out [5] that d is also the minimal period of $B(n) \pmod p$. Montgomery et al. [9] gave convincing heuristics to the truth of the conjecture and established the conjecture for new prime numbers after deep computations. This implies that the conjecture holds for all primes less than 126 as well as for the primes in $\{137, 149, 157, 163, 167, 173\}$. On the other hand, Car et al. [5] established the conjecture under some conditions on the p-adic digits of d. The link of r with the Bell numbers $B(n)$ modulo p (see [2, 3], [10]) is the following:

$$B(n) \equiv -\mathrm{Tr}(r^{c(p)})\mathrm{Tr}(r^{n-c(p)-1}) \pmod p. \tag{2}$$

Gallardo and Rahavandrainy [8] generalized the Bell numbers $B(n)$ in $\mathbb{F}_p$ to some rational fraction of r, $\beta(n) \in \mathbb{F}_q$, with the property that $\mathrm{Tr}(\beta(n)) = -B(n)$. Our contribution in the present paper is to extend the results in [5] in two manners. First, we consider conditions on the $p-1$ roots of r in $\mathbb{F}_q$ (as, e.g., $r^{c(p)}$) that implies the conjecture. Second, we consider several cases in which $d < g(p)$ holds (proving that this assumption is impossible), including the cases in which the base-p digits of d are all 1 (and similar cases), or the base-p digits of d are all small.

More precisely, our main result is as follows:

Theorem 1 *Let p be an odd prime number larger than 6. Write d in base p as follows $d = d_0 + d_1 p + \cdots + d_{p-1}p^{p-1}$ with $0 \le d_j \le p-1$ for all j. Put $m_0 = d_0$ and $m_k = d_1 + \cdots + d_k$, for $k = 1, \ldots, p-2$. The following statements hold.*

(a) Let $c_1(p) = m_0 + m_1 p + m_2 p^2 + \cdots + m_{p-2}p^{p-2}$. Assume that $r^{c_1(p)} = r^{1+c(p)+p^{p-1}-p^p}$. Then $d = g(p)$.

(b) Assume that $d < g(p)$. Then $d_1 = 1$ implies that $d_{p-3} = 0$.

(c) If for some integer a such that $0 < a \le p$ we have $d = \frac{p^a-1}{p-1}$ then $a = p$ and $d = g(p)$.

(d) Assume that $d < g(p)$, and let a be an integer such that $p-2 \le a \le p-1$. Then $d \ne 1 + a(p + p^2 + \cdots + p^{p-3} - p^j)$ when $j = p-6$.

(e) Assume that $d < g(p)$. Let $D_k = \sharp\{j\colon d_j = k\}$ be the number of j's for which $d_j = k$. Assume that $D_2 \not\equiv D_0 \pmod 2$ and that $2D_0 + D_1 \ne D_3$. Then it is impossible that $d_j \in \{0, 1, 2, 3\}$ for all $j = 0, \ldots, p-1$.

In order to describe more explicitly some of our results in the theorem, we work some examples in which we chose an explicit prime number p.

- We take $p = 3$. Consider the hypothesis (a) and (c) of the theorem. We have $d = d_0 + 3d_1 + 9d_2$ where $d_0, d_1, d_2 \in \{0, 1, 2\}$. Furthermore, we have also $m_0 = d_0$, and $m_1 = d_1$. Observe that $g(3) = \frac{3^3-1}{3-1} = 13$, and that $c(3) = 1 + 2 \cdot 3 = 7$. Moreover,

$$r^{c_1(3)} = r^{1+c(3)+3^2-3^3} = r^{8-18} = r^{-10}. \tag{3}$$

  Furthermore, we have $r^{13} = 1$, since the minimal period d of $B(n)$ modulo 3 is the order of r, and $r^{g(3)} = 1$. In the following, we still have $p = 3$.

- Let us prove (a): Since d divides $g(3) = 13$ and $d > 1$, we get immediately that $d = 13 = g(3)$. But let come to the same result directly. Assume to the contrary that $d < g(3)$. We claim that

$$d_2 = 0. \tag{4}$$

In order to prove the claim, observe that if $d_2 > 0$ then $d = d_0 + 3d_1 + 9d_2 > 9$. But $d < 13$ since $g(3) = 13$. This is impossible since d must divide 13. This proves the claim. We have by hypothesis, and by (3)

$$r^{d_0+3d_1} = r^{d_0+d_1 p} = r^{m_0+m_1 p} = r^{c_1(p)} = r^{c_1(3)} = r^{-10} = r^3. \tag{5}$$

In other words, (5) says that $r^{d_0+3d_1-3} = 1$. Observe that (4) implies that $d_0 + 3d_1 - 3 = d - 3$. Thus, d divides $d-3$. Thus, the only possibility left is that $d-3 = 0$. But this means that $d = 3$, and clearly 3 does not divide 13.

- Let us prove (c). The hypothesis read

$$d \in \{\frac{3-1}{3-1}, \frac{3^2-1}{3-1}, \frac{3^3-1}{3-1}\} = \{1, 4, 13\}$$

when a takes the values $1, 2, 3$ respectively. We reject $d = 1$ since $r \neq 1$. We reject $d = 4$ since d must divide $g(3) = 13$.

We also have a numerical result about the problem of how large can be d. We consider the special case in which $d = g(p)/(2p+1)$, that is, the maximal possible value of d when $d < g(p)$. In this case, $p > 3$ and $2p+1$ are both primes, so that $p \equiv 1 \pmod 4$ and p belong to the sequence $A103579$ (minus the first term) of the OEIS [12], namely,

$$p \in \{5, 29, 41, 53, 89, 113, 173, 233, 281, 293, 509, 593, 641, 653, 761, 809, \ldots\}.$$

Observe that Lemma 2 does not dismiss $g(p)/(2p+1)$ to be equal to d.

Theorem 2 *For any odd prime p such that $2p+1$ is also prime, $p \equiv 1 \pmod 4$, and $p < 100000$, we have $d \neq g(p)/(2p+1)$.*

Remark 1 *Montgomery et al. [9, Theorem 2.1] proved that for any odd prime p for which $2p+1$ is also prime, $2p+1$ divides $g(p)$ if and only if $p \equiv 1 \pmod 4$. It is also clear [5, Lemma 1.1] (for any odd prime p) that if $2p+1$ divides $g(p)$ then $2p+1$ is prime.*

We discuss a special case of Theorem 2 as an example.

- We consider the case when $p = 5$. This is the minimal possible value of p. We have $g(5) = \frac{5^5-1}{5-1} = 781 = 11 \cdot 71$. We want to prove that $d \neq g(5)/(2 \cdot 5 + 1) = 71$. Assume, on the contrary, that $d = 71$. We will compute r^{71} in the following manner. We know that $r^5 = r + 1$. We write d in base 5 (radix-5 expansion of d) as follows: $d = g(5)/11$, with

$$g(5) = 1 + 1 \cdot 5 + 1 \cdot 5^2 + 1 \cdot 5^3 + 1 \cdot 5^4,$$

and

$$11 = 1 + 2 \cdot 5.$$

Dividing the 5-adic number $g(5) + O(5^5)$ by the 5-adic number $1 + 2 \cdot 5 + O(5^5)$ we get

$$d + O(5^5) = 1 + 4 \cdot 5 + 2 \cdot 5^2 + O(5^5).$$

This really means that $71 = d = 1 + 4 \cdot 5 + 2 \cdot 5^2$. This allows us to compute

$$r^{71} = r \cdot (r+1)^4 \cdot (r+2)^2,$$

since $r^5 = r + 1$ and $r^{5^2} = r + 2$. Expanding and collecting we obtain after some computation

$$r^{71} = 4 \cdot r^4 + 2 \cdot r^3 + 4 \cdot r^2 + 3 \cdot r + 1.$$

Therefore, $r^{71} \neq 1$, and we obtain our result.

Below, in section 2, we prove some results useful for the proof of Theorem 1. We believe that these results might have an interest in themselves.

Throughout the paper, we put

$$d = d_0 + d_1 p + \cdots + d_{p-1} p^{p-1} \tag{6}$$

the radix-p expansion of d, the order of r in $\mathbb{F}_q$ (i.e., we have $0 \leq d_j \leq p-1$ for all j).

2 Tools

The following lemma is [5, Lemma 1.1 (b)]

Lemma 1 *Every divisor δ of $g(p)$ is of the form $\delta = 2kp+1$ for some non-negative integer k.*

The next result is [5, Lemma 3.1]

Lemma 2 *With d as in (6), if $d < g(p)$, then $d_0 = 1$ and $d_{p-2} = d_{p-1} = 0$.*

The next result is [5, Theorem 3.5 (b)].

Lemma 3 *Assume that $d < g(p)$. Then*

$$2p - 1 \leq d_0 + d_1 + \cdots + d_{p-1} < p^2 - 3p.$$

The following lemma [8, Lemma 7] is about the $p-1$ roots of r.

Lemma 4 *The set of $y \in \mathbb{F}_q$ such that $y^p = ry$ equals $\{kr^{c(p)} : k \in \mathbb{F}_p\}$*

We also have the following:

Lemma 5 *Let $y = r^{c(p)}$. Then*

(a) The order of y is equal to d. In particular, we have that $y^d = 1$.

(b) $y^{d-s-1} = r^s (r+1)^{s-d_1} (r+2)^{s-(d_1+d_2)} + \cdots + (r+p-2)^{s-(d_1+\cdots+d_{p-2})}$, where $s = d_1 + \cdots + d_{p-1}$.

Proof. Since $c(p) = \frac{p^p - g(p)}{p-1}$ it follows that $c(p)(p-1) = g(p)(p-2)+1$. Thus $\gcd(c(p), g(p)) = 1$. Therefore, $\gcd(c(p), d) = 1$ since d divides $g(p)$. We have then

$$\mathrm{o}_p(y) = \frac{\mathrm{o}_p(r)}{\gcd(\mathrm{o}_p(r), c(p))} = \frac{d}{1} = d.$$

This proves (a). In order to prove (b) observe that Lemma 2 implies that $d_0 = 1$. Thus, one has

$$y^d = y (y^p)^{d_1} \cdots (y^{p^{p-1}})^{d_{p-1}}. \tag{7}$$

By Lemma 4 we have that $y^p = ry$, and hence we obtain

$$(y^p)^{d_1} = r^{d_1} y^{d_1}, \tag{8}$$

$$(y^{p^2})^{d_2} = ((ry)^p)^{d_2} = (r^p y r)^{d_2} = (r+1)^{d_2} y^{d_2} r^{d_2} = r^{d_2} (r+1)^{d_2} y^{d_2}. \tag{9}$$

Analogously, we obtain, for $3, \ldots, p-1$:

$$(y^{p^3})^{d_3} = r^{d_3} (r+1)^{d_3} (r+2)^{d_3} y^{d_3}, \ldots, \tag{10}$$

$$(y^{p^{p-1}})^{d_{p-1}} = r^{d_{p-1}} (r+1)^{d_{p-1}} \cdots (r+p-2)^{d_{p-1}} y^{d_{p-1}}. \tag{11}$$

Putting (8),(9),(10),(11) into (7) we get the result. ■

The next result follows from [13].

Lemma 6 *One has that $d > 2^{2.54 \cdot p}$.*

3 Proof of Theorem 1

In order to prove (a) observe that we have $y = r^{c(p)}$. Thus, $y^d = 1$ by Lemma 5 (a). Hence, Lemma 5 (b) implies that

$$1 = y^d = r^s(r+1)^{s-m_1}\cdots(r+p-2)^{s-m_{p-2}}y^{s+1}, \tag{12}$$

where $s = m_{p-1}$. Observe that since $d_0 = 1$ (see Lemma 2) we have

$$r^{c_1(p)} = r(r+1)^{m_1}(r+2)^{m_2}\cdots(r+p-2)^{m_{p-2}}. \tag{13}$$

Multiply both sides of (12) by $r^{c_1(p)}$ to get

$$r^{c_1(p)} = r^{s+1}(r+1)^s\cdots(r+p-2)^s y^{s+1}. \tag{14}$$

We also write (14) as

$$r^{c_1(p)} = \frac{ry^{s+1}}{(r+p-1)^s}(r(r+1)\cdots(r+p-1))^s. \tag{15}$$

We have $r(r+1)\cdots(r+p-1) = 1$ since $r^{g(p)} = 1$. Thus, (15) implies

$$r\cdot y^{s+1} = (r+p-1)^s\cdot r^{c_1(p)}. \tag{16}$$

Remember that we assume that $r^{c_1(p)} = r^{1+c(p)+p^{p-1}-p^p}$. One has $r^{p^p} = 1$ since $g(p)$ divides p^p-1. Moreover, we have $r^{p^{p-1}} = r+p-1$. Thus, we obtain

$$r^{c_1(p)} = r\cdot y\cdot r^{p^{p-1}}\cdot r^{-p^p} = r(r+p-1)y. \tag{17}$$

Hence, (16) and (17) imply

$$y^s = (r+p-1)^{s+1}. \tag{18}$$

Applying the Frobenius over (18) (i.e., using that $y^p = ry$) we get

$$r^s y^s = r^{s+1}. \tag{19}$$

Thus, (18) says that

$$y^s = r. \tag{20}$$

All d_j are equal to 1 when $d = g(p)$. Thus, $s = p-1$ and (20) is trivially true. Assume that $d < g(p)$. Write (20) as:

$$y^{s-(p-1)} = 1. \tag{21}$$

It follows from (21) that the order of y divides $s-(p-1)$. In other words, by Lemma 5 (a) we have that:

$$d \mid s-(p-1). \tag{22}$$

By Lemma 3 we obtain that $s-1 \geq 2p-2$. Thus, $s \neq p-1$. Lemma 3 implies that s is small, indeed one has that $s \leq p(p-3)-1$. Thus, (22) is impossible by Lemma 6. This proves the result.

In order to prove (b) put $e = g(p)/d$. Observe first that Lemma 1 implies that one has for positive integers K, k, and ℓ: $g(p) = 2Kp+1, d = 2kp+1$, and $e = 2\ell p+1$. Hence,

$$2Kp+1 = g(p) = de = (2kp+1)(2\ell p+1). \tag{23}$$

We rewrite (23) as follows:

$$2K = 4k\ell p + 2k + 2\ell. \tag{24}$$

By Lemma 2 one has $d = 1+d_1p+\cdots+d_{p-3}p^{p-3}$. Observe that

$$2K = \frac{g(p)-1}{p} = 1+p+\cdots+p^{p-2}, \tag{25}$$

and that

$$2k = \frac{d-1}{p} = d_1 + \cdots + d_{p-3}p^{p-4}. \tag{26}$$

Thus, (24), together with (25) and (26) says that

$$1 + p + \cdots + p^{p-2} = 2\ell p \cdot 2k + 2k + 2\ell = 2\ell p(d_1 + \cdots + d_{p-3}p^{p-4}) + d_1 + \cdots + d_{p-3}p^{p-4} + 2\ell. \tag{27}$$

Assume that $d_1 = 1$. Reduce (27) modulo p to get the following:

$$p \mid \ell. \tag{28}$$

This implies that $\ell \geq p$. Thus, (27) implies that

$$1 + p + \cdots + p^{p-3} + p^{p-2} \geq 2p^2 d_{p-3}p^{p-4} = 2d_{p-3}p^{p-2} \geq 2p^{p-2}, \tag{29}$$

assuming that $d_{p-3} \neq 0$. But

$$p^{p-2} > p^{p-2} - 1 \geq \frac{p^{p-2}-1}{p-1} = 1 + p + \cdots + p^{p-3}. \tag{30}$$

This contradicts (29). Thus, $d_{p-3} = 0$. This proves (b).

In order to prove (c) assume, on the contrary, that for $1 < a < p$ one has

$$d = \frac{p^a - 1}{p-1} = 1 + p + \cdots + p^{a-1}. \tag{31}$$

In particular, we have that $d < g(p)$. We get from (31) that the sum $S = \sum_{j=0}^{a} d_j$ of digits of d satisfies $S = a \leq p-1$. But by Lemma 3 we know that $S \geq 2p-1$. This is impossible. This proves the result.

In order to prove (d) by contradiction, let us write the radix-p expansion of d as follows

$$d = 1 + ap + \cdots + ap^{j-1} + ap^{j+1} + \cdots + ap^{p-3}. \tag{32}$$

We have

$$h_1 = r^{1+ap+\cdots+ap^{j-1}} = r(r+1)^a \cdots (r+p-7)^a, \tag{33}$$

$$h_2 = r^{ap^{j+1}+\cdots+ap^{p-1}} = (r+p-5)^a \cdots (r+p-1)^a. \tag{34}$$

Put $h = r^{a-1}(r+p-6)^a$. Since $hh_1h_2 = (r^p - r)^a = 1$ in $\mathbb{F}_q$, and $1 = r^d = h_1h_2$, we have $h = 1$. In other words, we have the following:

$$r^{a-1}(r+p-6)^a = 1. \tag{35}$$

But (35) says that

$$r^{a-1+ap^{p-6}} = r^{a-1}(r+p-6)^a = 1. \tag{36}$$

Hence,

$$d \mid a - 1 + ap^{p-6}. \tag{37}$$

But $d > p^{p-3}$, thus (37) is impossible. This proves (d).

In the following, we use repeatedly the simple fact:

If $\deg(A(x)) < p$ and $\deg(B(x)) < p$ then the equality

$$A(r) = B(r) \tag{38}$$

is impossible, since the minimal polynomial of r, namely, $x^p - x - 1$ has degree p.

In order to prove (e) assume (to the contrary) that $d_j \in \{0, 1, 2, 3\}$ for all $j = 0, \ldots, p-1$. Thus, we have the equality of sets:

$$\{j \colon d_j \neq 0\} = \{j \colon d_j = 1\} \cup \{j \colon d_j = 2, 3\} \tag{39}$$

Observe that we have

$$\prod_{j=0}^{p-1}(r+j) = r^p - r = 1, \tag{40}$$

and that the equation $r^d = 1$ can be written as

$$\prod_{\{j\colon d_j\neq 0\}}^{p-1}(r+j)^{d_j} = \prod_{j=0}^{p-1}(r+j)^{d_j} = 1 \tag{41}$$

since $(r+j)^{d_j} = 1$ when $d_j = 0$.

Hence, we have by (39)

$$\prod_{\{j\colon d_j=1\}}^{p-1}(r+j)\cdot\prod_{\{j\colon d_j=2,3\}}^{p-1}(r+j)^{d_j} = \prod_{\{j\colon d_j\neq 0\}}^{p-1}(r+j)^{d_j} = 1. \tag{42}$$

Multiply both sides of (42) by $M = \prod_{\{j\colon d_j=0,2,3\}}^{p-1}(r+j)$ to get

$$M\cdot\prod_{\{j\colon d_j=1\}}^{p-1}(r+j)\prod_{\{j\colon d_j=2,3\}}^{p-1}(r+j)^{d_j} = M. \tag{43}$$

But (40) implies that

$$M\cdot\prod_{\{j\colon d_j=1\}}^{p-1}(r+j) = \prod_{\{j\colon d_j=0,1,2,3\}}^{p-1}(r+j) = \prod_{j=0}^{p-1}(r+j) = 1, \tag{44}$$

so that (43) says that

$$\prod_{\{j\colon d_j=2,3\}}^{p-1}(r+j)^{d_j} = M = \prod_{\{j\colon d_j=0,2,3\}}^{p-1}(r+j). \tag{45}$$

Dividing both sides of (45) by $\prod_{\{j\colon d_j=2,3\}}^{p-1}(r+j)$ we obtain

$$\prod_{\{j\colon d_j=2,3\}}^{p-1}(r+j)^{d_j-1} = \prod_{\{j\colon d_j=0\}}^{p-1}(r+j). \tag{46}$$

But (46) can also be written as

$$\prod_{\{j\colon d_j=2\}}^{p-1}(r+j)\cdot\prod_{\{j\colon d_j=3\}}^{p-1}(r+j)^2 = \prod_{\{j\colon d_j=0\}}^{p-1}(r+j) \tag{47}$$

since when $d_j = 2$ in (46) then $d_j - 1 = 1$ in the exponent of $(r+j)$ in (47), and when $d_j = 3$ in (46) then $d_j - 1 = 2$ in the exponent of $(r+j)$ in (47).

Case 1. Assume that

$$D_2 + 2D_3 < p. \tag{48}$$

Since $D_0 < p$ as well, it follows from (48) that both the polynomial $P(r)$ on the left-hand side of (47), and the polynomial $Q(r)$ on the right-hand side of (47), have degree less than p. By hypothesis, they have different degree. Namely, $\deg(P(r)) = D_2 + 2D_3 \neq D_0 = \deg(Q(r))$, since D_2 and D_0 have different parity. But $P(r) - Q(r) = 0$ in $\mathbb{F}_q$. This is impossible since the minimal polynomial of r has degree p (see (38)).

Thus, it remains to consider the case:

Case 2. Assume that

$$D_2 + 2D_3 \geq p. \tag{49}$$

Proceed now as before, (see steps (43), (44), (45), (46),(47)) but with

$$N = \prod_{\{j\,:\,d_j=0\}}^{p-1} (r+j) \cdot \prod_{\{j\,:\,d_j=1\}}^{p-1} (r+j), \tag{50}$$

instead of M. Namely, multiply both sides of (47) by N and use (40) to obtain the analogue of (47):

$$\prod_{\{j\,:\,d_j=0\}}^{p-1} (r+j)^2 \cdot \prod_{\{j\,:\,d_j=1\}}^{p-1} (r+j) = \prod_{\{j\,:\,d_j=3\}}^{p-1} (r+j). \tag{51}$$

Sub-case $2A$: Assume that

$$D_1 + 2D_0 < p. \tag{52}$$

Since $D_3 < p$ and (52) hold, it follows from (51) that both the polynomial $P_1(r)$ on the right-hand side of (47), and the polynomial $Q_1(r)$ on the left-hand side of (51), have degree less than p. By hypothesis, they have different degree. Namely, $\deg(P_1(r)) = D_1 + 2D_0 \neq D_3 = \deg(Q_1(r))$. But $P_1(r) - Q_1(r) = 0$ in $\mathbb{F}_q$. This is impossible since the minimal polynomial of r has degree p (see again (38)).

Thus, it remains to consider the following case.

Sub-case $2B$: Assume that

$$D_1 + 2D_0 \geq p. \tag{53}$$

We assume then that (49) and (53) hold simultaneously. This implies, by adding these inequalities, that

$$D_0 + D_3 + (D_0 + D_1 + D_2 + D_3) \geq 2p. \tag{54}$$

But $D_0 + D_1 + D_2 + D_3 = p$ since all d_j, for $j = 0, \ldots, p-1$, belong to $\{0, 1, 2, 3\}$. Therefore, (54) says that:

$$D_0 + D_3 \geq p. \tag{55}$$

But on the other hand,

$$D_0 + D_3 < D_0 + D_1 + D_2 + D_3 = p, \tag{56}$$

with a strict inequality in (56) since $d_0 = 1$ implies that $D_1 \geq 1$. This contradiction proves (e), thereby finishing the proof of the theorem.

Remark 2 *Using similar arguments we can show, for (a), that if $d_{p-3} = 0$ then we must have $2\ell \geq p$. Similarly, for (d), the cases $j \in \{p-5, p-4\}$ can be handled by a similar method. Observe that our argument requires that $j \geq p-6$. Concerning (e), observe that by symmetry we can alternatively ask that $D_1 \not\equiv D_3 \pmod 2$ and $2D_3 + D_2 \neq D_0$, in order to get the same contradiction.*

4 Proof of Theorem 2

The result follows from running a straightforward gp-PARI computer program. The program took about 14 days to check all these primes p. In all cases, we obtained that $r^d \neq 1$ in $\mathbb{F}_q$ when $d = \frac{g(p)}{2p+1}$. The first 162 primes, corresponding to $p < 20000$, were checked in about 7 minutes. We wrote the program based on the following. By [9, Theorem 2.1] $2p+1$ divides $g(p)$. Assume, on the contrary, that $d = g(p)/(2p+1)$. Computing the quotient of the p-adic number $g(p) + O(p^p)$ divided by $1 + 2p + O(p^p)$, we obtain the radix-p expansion of d, say $d = 1 + d_1 p + \cdots + d_{p-1} p^{p-1}$. As a next step, we compute $r^d = r(r+1)^{d_1} \cdots (r+p-1)^{p^{p-1}}$ in $\mathbb{F}_q$ by using the finite sequence $s_1 = r$, $s_{n+1} = s_n \cdot (r+n)^{d_n}$. Finally, we checked if $r^d \neq 1$ in $\mathbb{F}_q$. This holds. Since this is impossible, we obtain the result.

Acknowledgment. We are grateful to the referee for detailed comments and suggestions. Thanks to his (her) work, the actual paper is substantially better.

References

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

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

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

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

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

[6] R. E. Dalton and J. Levine, Minimum periods, modulo p, of first order Bell exponential integers, Math. Comp., 16(1962), 416–423.

[7] M. d'Ocagne. Sur une classe de nombres remarquables, Amer. J. Math., 9(1887), 353–380.

[8] L. H. Gallardo and O. Rahavandrainy, Bell numbers modulo a prime number, traces and trinomials, Electron. J. Combin., 21(2014), 30 pp.

[9] P. Montgomery, S. Nahm and S. S. Wagstaff, The period of the Bell numbers modulo a prime. Math. Comp., 79(2010), 1793–1800.

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

[11] 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), 879–882.

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

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

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