Bull. Korean Math. Soc. **45** (2008), No. 1, pp. 143–155

# ABOUT THE PERIOD OF BELL NUMBERS MODULO A PRIME

Mireille Car, Luis H. Gallardo, Olivier Rahavandrainy, and Leonid N. Vaserstein

Abstract. Let $p$ be a prime number. It is known that the order $o(r)$ of a root $r$ of the irreducible polynomial $x^p - x - 1$ over $\mathbb{F}_p$ divides $g(p) = \frac{p^p-1}{p-1}$. Samuel Wagstaff recently conjectured that $o(r) = g(p)$ for any prime $p$. The main object of the paper is to give some subsets $S$ of $\{1, \ldots, g(p)\}$ that do not contain $o(r)$.

## 1. Introduction

Some simple results about $g(p)$ are collected in the following lemma:

**Lemma 1.1.** *Let $p$ be an odd prime number and set $g(p) = \frac{p^p-1}{p-1}$. Then*

a) $\gcd(p-1, g(p)) = 1$, *indeed* $g(p) \equiv 1 \pmod{p(p-1)}$, *and* $g(p) \equiv 1 \pmod 4$.

b) *Every divisor $d$ of $g(p)$ is of the form $d = 2kp + 1$ for some integer $k \geq 0$.*

c) *Every divisor $d$ of $g(p)$ is of the form $d = 4kp + 1$ for some integer $k \geq 0$ when $p \equiv 3 \pmod 4$.*

*Proof.* We prove only c), the rest is well known and it is easy to check. Since $(2kp+1)(2hp+1) = 2(2khp + k + h)p + 1$, we may assume that $d = 2kp+1$ is a prime divisor of $g(p)$. Write $p = g^m$, where $g$ is a generator of the cyclic group $C(d)$ of nonzero elements of $\mathbb{Z}/d\mathbb{Z}$. But $d$ divides $p^p - 1 = (p-1)g(p)$ so that $p^p \equiv 1 \pmod d$. In other words we have:

$$g^{pm} \equiv 1 \pmod d.$$

Thus, the order $o(g) = d - 1 = 2kp$ of $g$ in $C(d)$ satisfies: $o(g)$ divides $pm$. It follows that $2k$ divides $m$ so that $m$ is even. This proves that $p$ is a square modulo $d$. Trivially, $d$ is a square modulo $p$ since $d \equiv 1 \pmod p$. Now, by the

Received July 30, 2007.

2000 *Mathematics Subject Classification.* 11B73, 11T06, 11T55.

*Key words and phrases.* Bell numbers modulo a prime, extension of prime degree p of $\mathbb{F}_p$.

quadratic law of reciprocity of Gauss we get:

$$1 = \left(\frac{d}{p}\right)\left(\frac{p}{d}\right) = (-1)^{(\frac{p-1}{2})(kp)} = (-1)^{(\frac{p-1}{2})k}$$

that proves the result. □

The Bell numbers $B(n)$ are given by the exponential generating function

$$\exp(e^x - 1) = \sum_{n=0}^{\infty} \frac{B(n)}{n!} x^n.$$

Let $p$ be a prime number. Set $b_p =$ the minimal period of $B(n)$ modulo $p$, $c_p =$ the order $o(r)$ of a root $r$ of the irreducible polynomial $f(x) = x^p - x - 1$ over $\mathbb{F}_p$, $d_p =$ the minimal number $g \geq 0$ such that $B(n) + \cdots + B(n+g) = 0 \pmod{p}$.

Some well known facts are proved (or are easily deduced) from: [6] and its bibliography, [3, pp. 84–91, Theorem 3.63, p.117, pp. 124–131, Theorem 3.84], [1, Exercise 9, pp. A V.158–A V. 159], [5] and [2]. Item c) is proved in [4]:

**Proposition 1.2.** *Let $p$ be a prime number and set $g(p) = \frac{p^p-1}{p-1}$. Then*

a) $b_p = c_p = d_p$.
b) $c_p$ *divides* $g(p)$.
c) $\frac{1}{2}\binom{2p}{p} \leq c_p$.
d) $c_p = g(p)$ *for* $p < 102$ *and also for* $p \in \{113, 163, 167, 173\}$.
e) *Every irreducible factor of* $F(x) = x^{g(p)} - x - 1 \in \mathbb{F}_p[x]$ *has degree* $c_p$. *So,* $F(x)$ *is irreducible if and only if* $c_p = g(p)$.
f) $c_p = g(p)$ *if and only if for any primitive element* $a \in \mathbb{F}_p$, *the trinomial* $f(x,a) = x^p - x - a \in \mathbb{F}_p[x]$ *is a primitive polynomial.*

We may also consider the conjecture that $c_p = g(p)$ in the following form: Let $d$ be a divisor of $g(p)$, and let $r$ be a root in $\mathbb{F}_{p^p}$ of $f(x) = x^p - x - 1$. Write $d$ in base $p$ as follows:

$$d = d_0 + \cdots + d_{p-1}p^{p-1},$$

where $0 \leq d_i \leq p-1$. Let $P(x) = x^{d_0}(x+1)^{d_1} \cdots (x+p-1)^{d_{p-1}} - 1$.
Then $c_p = o(r) = g(p)$ if and only if the unique solutions of the exponential equation

$$0 = r^{d_0}(r+1)^{d_1} \cdots (r+p-1)^{d_{p-1}} - 1 = P(r). \tag{1}$$

occur when $d_0 = d_1 = \cdots = d_{p-1}$.

While in [4] they do not consider the root $r$ in their proof, their proof of the lower bound c) in Lemma 1.2 comes essentially (besides a combinatorial counting argument) from the observation that equation (1) has the only solution $d_i = 0$ for all $i$ when

$$\delta = d_0 + d_1 + \cdots + d_{p-1} = \deg(P(x)) < p.$$

A slight improvement of the lower bound is:

**Proposition 1.3.** *Let $p > 3$ be a prime number. Then*

$$c_p \geq \frac{1}{2}\binom{2p}{p} + p.$$

*While,*

$$c_p \geq \frac{1}{2}\binom{2p}{p} + 3p,$$

*when $p \equiv 3 \pmod 4$.*

*Proof.* By using the known lower bound $s = \frac{1}{2}\binom{2p}{p}$ in Proposition 1.2 c) we have just to prove that our candidates satisfy the right congruence conditions: A theorem of Kummer says that the exponent of a prime divisor $q$ in $\binom{n+k}{k}$ is the number of carries needed to add $n$ and $k$ when each of them is written in base $q$. It follows that for odd $n > 1$, $\frac{1}{2}\binom{2n}{n}$ is always even and that if $n > 3$ and $n \equiv 3 \pmod 4$ then one has $\binom{2n}{n} \equiv 0 \pmod 8$. Moreover, for any prime $p$ it is known that $\binom{2p}{p} \equiv 2 \pmod p$. We have then proved that $s \equiv 0 \pmod 2$, that $s \equiv 0 \pmod 4$ when $p > 3$ is congruent to 3 modulo 4, and that $s \equiv 1 \pmod p$. The result follows then from Proposition 1.2 b) and from Lemma 1.1. □

The next section has to do with version f) (see Proposition 1.2) of the conjecture:

## 2. Improvement on Theorem 3.84 of Lidl and Niederreiter's book

The object of the section is to prove the following result that improves on the theorem in the title.

**Theorem 2.1.** *Let $p$ be a prime number and let $a \in \mathbb{F}_p$ be a primitive element. Let $r \in \mathbb{F}_{p^p}$ be a root of $f(x) = x^p - x - 1$ of order $o(r)$. Then the trinomial $f(x,a) = x^p - x - a \in \mathbb{F}_p[x]$ has order equal to $o(r)(p-1)$.*

Let $s$ be a root in $\mathbb{F}_{p^p}$ of $f(x,a)$. The following lemma proves Theorem 2.1 and describes in detail some natural invariants associated to $s$:

**Lemma 2.2.** *Let $p$ be a prime number and let $a \in \mathbb{F}_p$ be a primitive element. Let $s$ be a root in $\mathbb{F}_{p^p}$ of $f(x,a) = x^p - x - a$. Let $e(a)$ be the least positive integer $g$ such that $s^g \in \mathbb{F}_p$; $e(a)$ is usually called the "integral" order of $f(x,a)$. Let $h(a)$ be the least positive integer $h$ such that $s^h = a$. Set $r = s/a$ a root of $f(x) = x^p - x - 1$. Set $d = o(r)$, the order of $r$ and as before set $g(p) = \frac{p^p-1}{p-1}$. Then*

a) *For any primitive $a$ one has $e(a) = d$.*
b) *$h = h(a)$ does not depends on $a$.*
c) *$d$ divides $h$ and $h \leq g(p)$.*
d) *$h \equiv 1 \pmod{p-1}$.*
e) *$o(s) = (p-1)o(r)$.*

f) *$s$ is never a power of $r$ while: Let the positive integers $u \leq p^p$ and $w \leq g(p)$ be such that $d(p-1) \mid u-1$ and $d \mid w$ and $p-1 \mid w-1$. Then $p-1 \mid u-w$, $\gcd(\frac{u-w}{p-1}, d) = 1$ and*

$$r = s^{u-w}.$$

*Specific values of $u, w$ are: $u \in \{p^p, h(p-1)+1\}$ and $w \in \{g(p), h\}$.*

g) *There exist explicit solutions to the equation $r = \gamma^{p-1}$.*

*Proof.* First of all observe that $a^{g(p)} \equiv aa^p \cdots a^{p^{p-1}} \equiv a^p \equiv a \pmod p$. Analogously we have in $\mathbb{F}_{p^p}$: $r^{g(p)} = r(r+1)\cdots(r+p-1) = r^p - r = 1$ so that $s^{g(p)} = a^{g(p)} = a$. This proves that $e(a)$ and $h(a)$ are well defined, that $e(a)$ divides $g(p)$, that $h(a) \leq g(p)$ and that $e(a)$ divides $h(a)$. Now, consider $r^d = 1$, i.e., $s^d = a^d \in \mathbb{F}_p$. This proves that $e(a)$ divides $d$. Set $s^{e(a)} = b \in \mathbb{F}_p$. By [3, Lemma 3.17, p. 89] one has that the order $o(s)$ of the root $s$, satisfy $o(s) = e(a)o(b)$, where $o(b)$ is the order of $b$ in $\mathbb{F}_p^*$. Set $h(a) = Ke(a)$ for some integer $K$. Now, by definition of $h(a)$ we have $s^{Ke(a)} = s^{h(a)} = a$ so that $a = b^K$. But, $a$ is primitive, so $b$ is also primitive so that

$$\gcd(p-1, K) = 1.$$

One gets:

$$o(s) = (p-1)e(a). \tag{2}$$

Taking norms in both sides of $a = s^{h(a)}$ one gets $a = a^{h(a)}$, i.e.,

$$h(a) \equiv 1 \pmod{p-1}.$$

In other words:

$$p - 1 \mid e(a)K - 1.$$

Set $b = a^L$ for some integer $L$ coprime with $p-1$. It is not difficult to see that we have $a = a^{LK}$ in $\mathbb{F}_p$ so that

$$p-1 \mid LK - 1.$$

It follows that

$$e(a)K \equiv LK \pmod{p-1}$$

i.e., that

$$e(a) \equiv L \pmod{p-1}. \tag{3}$$

Now, from (3) and by definition of $L$ and of $e(a)$ it becomes clear that

$$s^{e(a)} = a^{e(a)}.$$

In other words we have $r^{e(a)} = 1$. But this proves that $d = o(r)$ divides $e(a)$. We conclude that for all primitive $a$ one has:

$$e(a) = d.$$

In particular $h(a) = Kd$ so that $d$ divides $h(a)$. It follows from (2) that

$$o(s) = (p-1)o(r). \tag{4}$$

It remains to prove that $h(a)$ does not depends on the value of the primitive $a$ : We can assume that $s/a = r = t/b$ where $t^p = t + b$ for some primitive $b \in \mathbb{F}_{p^p}$. Set $b = a^L$ for some $L$. From the definitions of $h(a)$ and $h(b)$ we get:

$$a^{Lh(b)} s^{h(b)} = a^{h(b)+L}$$

so that

$$s^{h(b)} = a^{h(b)+L-Lh(b)} = a$$

since $h(b) \equiv 1 \pmod{p-1}$. This proves that $h(a) \leq h(b)$. The result b) follows by symmetry. We prove now f): Assume that $s = r^M$ for some positive integer $M$. Taking norms in boths sides of these equality we get the contradiction $a = 1$, thereby proving the first claim. In order to complete the proof, we just compute $s^{u-w}$, the other properties are clear:

$$s^{u-w} = \frac{r^u\, a^u}{r^w\, a^w} = \frac{r\, a}{1\, a} = r.$$

In order to prove g) observe that such $\gamma$ exist in $\mathbb{F}_{p^p}$ by Hilbert 90's Theorem. Since $\gcd(p-1, d) = 1$ there exists an integer $\phi$ such that $\phi(p-1) \equiv 1 \pmod{d}$. For any nonzero $a, c \in \mathbb{F}_p$ we may then take

$$\gamma = (ar)^\phi c.$$

Special cases are $\phi = \frac{u-w}{p-1}$, where $u, w$ are as in f), in particular when $u = p^p$ and $w = g(p)$ one has $\phi = 1 + 2p + 3p^2 + \cdots + (p-1)p^{p-2}$. □

## 3. The set of $d$'s with $d_0 + \cdots + d_{p-1} < 2p - 1$ does not contain $o(r)$

First of all we shall describe some properties that have the order $d = o(r)$ of $r$ assuming that it is strictly smaller that $g(p)$ :

**Lemma 3.1.** *Let $p$ be a prime number. Let $r \in \mathbb{F}_{p^p}$ be a root of $f(x) = x^p - x - 1$. Let $d = o(r)$ be the order of $r$. Write $d$ in base $p$ as follows*:

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

*Let $g(p) = \frac{p^p-1}{p-1}$. Assume that*

$$d < g(p).$$

*Then*

$$d_0 = 1, \quad d_{p-1} = 0 = d_{p-2}.$$

*Proof.* By Proposition 1.2 b) and from Lemma 1.1 we get $d_0 = 1$. Assume that $d_{p-1} \geq 1$. From Lemma 1.1

$$d(2ep + 1) = g(p)$$

for some integer $e \geq 1$. This implies the contradiction:

$$g(p) \geq (2p+1)d > dp \geq p^{p-1}\, p = p^p.$$

So, $d_{p-1} = 0$.

Assume now that $d_{p-2} \geq 1$. Analogously, there exist positive integers $K, k, e, l$ such that

$$g(p) = 2Kp + 1 = de = (2kp+1)(2lp+1).$$

Rewrite this as: $2K = 2(2k)lp + 2k + 2l$, i.e., as:

$$2K = 2(d_1 + \cdots + d_{p-2}p^{p-3})lp + (d_1 + \cdots + d_{p-2}p^{p-3}) + 2l.$$

From this we get the contradictory chain of inequalities:

$$2p^{p-2} > 2K \geq 2p^{p-3}p + p^{p-3} + 2 > 2p^{p-2}.$$

This proves that $d_{p-2} = 0$. □

The following corollary gives an upper bound for $d$ when $d < g(p)$ :

**Corollary 3.2.** *Let $p$ be an odd prime number. Let $\delta(p) = 4$ if $p \equiv 1 \pmod 4$ $\delta(p) = 2$ if $p \equiv 3 \pmod 4$. Let also $\mu(p) = 2$ if $p \equiv 1 \pmod 4$ and $\mu(p) = 4$ if $p \equiv 3 \pmod 4$.*

*Let*

$$B(p) = \frac{\delta(p)p^{p-2} - p^{p-3} + p + \delta(p)}{p^2 + \delta(p)p - 1}.$$

*Let $r \in \mathbb{F}_{p^p}$ be a root of $f(x) = x^p - x - 1$. Let $d = o(r)$ be the order of $r$. Assume that*

$$d < g(p).$$

*Then for some integer $k$ such that $\mu(p)k + 1 \geq B(p)$ one has*

$$d = p^{p-2} - (\mu(p)k+1)p + 1 \leq p^{p-2} - pB(p) + 1.$$

*Proof.* Clearly from Lemma 3.1 we obtain

$$d = d_0 + d_1p + \cdots + d_{p-3}p^{p-3} \leq 1 + (p-1)(p + \cdots + p^{p-4})$$

so that we have the upper bound $d \leq \delta_p$, where $\delta_p = 1 + p(p^{p-3} - 1)$. Observe that $\delta_p \equiv 1 \pmod{4p}$. Assume that for some integer $k \geq 0$ we have:

$$d = \delta_p - \mu(p)kp = p^{p-2} - (\mu(p)k+1)p + 1. \tag{5}$$

Observe that $d$ divides $p^p - 1$ so that $p^p \equiv 1 \pmod d$. Now reducing (5) modulo $d$ and multiplying both sides of the new equality by $-p^2$ we get

$$(\mu(p)k+1)p^3 - p^2 - 1 \equiv 0 \pmod d.$$

So, observing that $d$ is congruent to 1 modulo $p$, we get that for some positive integer $A > 0$ one has:

$$(\mu(p)k+1)p^3 - p^2 - 1 = (Ap-1)d. \tag{6}$$

This is equivalent to:

$$(\mu(p)k+1)(p^2 + Ap - 1) = Ap^{p-2} - p^{p-3} + A + p. \tag{7}$$

Now, reduce both sides of (7) modulo 4. We get $A \equiv 0 \pmod 4$ when $p \equiv 1 \pmod 4$ and $A \equiv 2 \pmod 4$ when $p \equiv 3 \pmod 4$. In particular, $A \geq \delta(p)$ so that from (6) we obtain the inequality

$$(\mu(p)k+1)p^3 - p^2 - 1 \geq (\delta(p)p-1)d.$$

Using (5), the result follows after some computation. □

The following lemma show some necessary conditions for (1) to hold:

**Lemma 3.3.** *Let $p$ be an odd prime number. Let $g(p) = \frac{p^p-1}{p-1}$. Let $d$ be a divisor of $p^p - 1$ and let $r$ be a root in $\mathbb{F}_{p^p}$ of $f(x) = x^p - x - 1$. Write $d$ in base $p$ as follows:*

$$d = d_0 + \cdots + d_{p-1}p^{p-1},$$

*where $0 \leq d_i \leq p-1$. Let $P(x) = x^{d_0}(x+1)^{d_1}\cdots(x+p-1)^{d_{p-1}} - 1$. Set $\delta = \deg(P(x))$.*

a) *Assume that $d$ divides $g(p)$, then $\gcd(\delta, p-1) = 1$ so that $\delta$ is odd.*

b) *Assume that $P(r) = 0$ and that not all $d_i$'s are equal. Then*

$$\delta \geq p + \sum_{\{j \mid d_j>0\}} 1.$$

*Proof.* By Lemma 1.1 a) $g(p)$ is coprime with $p-1$. The result a) follows then from $\delta \equiv d \pmod{p-1}$.

In order to prove b) we multiply both sides of (1) by $\prod_{\{i \mid d_i=0\}}(r+i)$ :

$$r^{e_0}(r+1)^{e_1}\cdots(r+p-1)^{e_{p-1}} = \prod_{\{i \mid d_i=0\}}(r+i), \tag{8}$$

where $e_i = 1$ if $d_i = 0$ and $e_i = d_i$ when $d_i > 0$. Now we divide both sides of (8) by $r(r+1)\cdots(r+p-1) = 1$ to get:

$$\prod_{\{j \mid d_j>0\}}(r+j)^{d_j-1} = \prod_{\{i \mid d_i=0\}}(r+i). \tag{9}$$

Consider now the polynomials of $\mathbb{F}_p[x]$ defined by

$$L(x) = \prod_{\{j \mid d_j>0\}}(x+j)^{d_j-1}, \quad R(x) = \prod_{\{i \mid d_i=0\}}(x+i).$$

Observe that not all $d_i = 0$, i.e., we have $\deg(R(x)) \leq p-1$ and that not all $d_i = 1$, i.e., we have $\deg(L(x)) > 0$. From the definition of $r$ and from (9) it follows that we have $\deg(L(x)) \geq p$. In other words we have $\sum_{\{j \mid d_j>0\}}(d_j - 1) \geq p$. This implies

$$\delta = \sum_{\{j \mid d_j>0\}} d_j \geq p + \sum_{\{j \mid d_j>0\}} 1$$

thereby proving the lemma. □

More information on $\delta$ is contained in the following crucial lemma:

**Lemma 3.4.** *Let $p$ be a prime number. Let $d$ be a divisor of $p^p-1$ and let $r$ be a root in $\mathbb{F}_{p^p}$ of $f(x)=x^p-x-1$. Write $d$ in base $p$ as: $d=d_0+\cdots+d_{p-1}p^{p-1}$, where $0\leq d_i\leq p-1$. Let $Tr$ denote the trace of $\mathbb{F}_{p^p}$ over $\mathbb{F}_p$. Assume that for some polynomial $A(x)\in\mathbb{F}_p[x]$ written $A(x)=a_0+a_1x+\cdots+a_nx^n$, one has*

$$P(x)=x^{d_0}(x+1)^{d_1}\cdots(x+p-1)^{d_{p-1}}-1=A(x)(x^p-x-1).$$

*Set $\delta=\deg(P(x))$ and set $n=\deg(A(x))$.*
*Then*

a) *$Tr(A(r))\equiv\delta\pmod p$.*
b) *One has in $\mathbb{F}_p$ :*

$$Tr(A(r))=(-1)\sum_{\{k\geq1\ \mid\ kp-1\leq n\}}a_{kp-1}.$$

*Proof.* By differentiating both sides of the equality $P(x)=A(x)(x^p-x-1)$ relative to $x$, we get

$$P'(x)=A'(x)(x^p-x-1)-A(x)$$

so that

$$A(r)=-P'(r). \tag{10}$$

On the other hand:

$$\frac{(P(x)+1)'}{P(x)+1}=\sum_i\frac{d_i}{x+i},$$

so that

$$P'(r)=\sum_i\frac{d_i}{r+i}. \tag{11}$$

From (10) and (11) we get

$$A(r)=-\sum_i\frac{d_i}{r+i}. \tag{12}$$

Observe that for all $i$

$$Tr(\frac{1}{r+i})=Tr(\frac{1}{r})=-1$$

since $x^p+x^{p-1}-1\in\mathbb{F}_p[x]$ is the minimal polynomial of $\frac{1}{r}$ and this polynomial has as roots all the $\frac{1}{r+i}$ for $i=0,\ldots,p-1$.

Now, take the trace in both sides of (12) to get in $\mathbb{F}_p$:

$$Tr(A(r))=-(\sum_i d_i(-1))=\sum_i d_i=\delta$$

that proves a).

In order to prove b) let define for each non-negative integer $k\geq0$ :

$$t_k=Tr(r^k).$$

Clearly one has in $\mathbb{F}_p$: $t_0 = p = 0$, and $t_1 = 0$ the coefficient of $x^{p-1}$ in $x^p - x - 1$. Observe that defining the $b_j$'s by:

$$\prod_{i=1}^{p}(x - (r+i)) = x^p - x - 1 = \sum_{j=0}^{p}(-1)^j\, b_j\, x^{p-j}$$

from Newton's identities

$$t_k = \sum_{i=1}^{k-1} b_i\, t_{k-i}(-1)^{i+1} + b_k\, k\,(-1)^{k+1}$$

one obtains:

$$t_2 = 0, \ldots, t_{p-2} = 0,\ t_{p-1} = -1.$$

Since $r^p = r + 1$ this repeats cyclically so that taking the trace in both sides of

$$A(r) = a_0 + a_1 r + \cdots + a_n r^n,$$

we get

$$Tr(A(r)) = -a_{p-1} - a_{2p-1} - \cdots$$

that proves b). □

Our main result follows:

**Theorem 3.5.** *Let $p$ be an odd prime number. Set $g(p) = \frac{p^p-1}{p-1}$. Let $r$ be a root in $\mathbb{F}_{p^p}$ of $f(x) = x^p - x - 1$ of order $o(r)$. Write a divisor $d$ of $p^p - 1$ in base $p$ as follows:*

$$d = d_0 + \cdots + d_{p-1}p^{p-1},$$

*where $0 \le d_i \le p-1$.*

a) *Assume that $r^d = 1$ and that not all $d_i$'s are equal. Then*

$$2p - 1 \le d_0 + \cdots + d_{p-1} \le p^2 - 3p + 1.$$

b) *Assume that $d = o(r) < g(p)$. Then*

$$p^2 - 3p > d_0 + \cdots + d_{p-1} \ge 2p - 1.$$

c) *Let $e$ be a divisor of $p^p - 1$ written in base $p$ as*

$$e = e_0 + \cdots + e_{p-1}p^{p-1},$$

*where $0 \le e_i \le p-1$. Assume that not all $e_i$'s are equal and that either $e_0 + \cdots + e_{p-1} < 2p - 1$ or that $e_0 + \cdots + e_{p-1} > p(p-3) + 1$. Then*

*$d$ does not divide $e$.*

*Proof.* One can write $r^d - 1 = 0$ in the form (1). Now from the equality in $\mathbb{F}_p[x]$ :

$$P(x) = x^{d_0}(x+1)^{d_1} \cdots (x+p-1)^{d_{p-1}} - 1 = A(x)(x^p - x - 1)$$

in which we set $n = \deg(A(x))$ and $\delta = \deg(P(x))$, we get

$$n = \delta - p = d_0 + \cdots + d_{p-1} - p.$$

Assume that $n < p-1$. Then by Lemma 3.4 one has

$$\delta \equiv 0 \pmod{p}$$

so that (observe that $d > 0$ and that $\delta < 2p-1$)

$$\delta = p.$$

By Lemma 3.3 one gets the contradiction

$$p = \delta \geq p + \sum_{\{j \mid d_j > 0\}} 1.$$

So one has

$$d_0 + \cdots + d_{p-1} \geq 2p-1.$$

Now, we have also that $r^{p^p-1-d} = 1$, so that:

$$(p-1) - d_0 + \cdots + (p-1) - d_{p-1} \geq 2p-1.$$

i.e., one has

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

that proves a). So, c) follows immediately also.

In order to prove b) observe that $d_0 = 1$ and $d_{p-1} = d_{p-2} = 0$ by Lemma 3.1 so that we can apply a). It remains just to prove the strict inequality $\delta < p^2 - 3p$. Assume that $\delta = p^2 - 3p + 1$. Set $M = \max(d_1, \ldots, d_{p-3})$. Using $d_0 = 1$ we get

$$\delta = p(p-3) + 1 \leq 1 + (p-3)M$$

i.e., we get the contradiction

$$p \leq M.$$

So, $\delta \leq p(p-3)$. Now by Lemma 3.3 a), one has that $\delta$ is odd. It follows that $\delta < p(p-3)$, thereby finishing the proof of the theorem. □

## 4. The set of $d$'s with at most 4 nonzero $d_i$'s does not contain $o(r)$

Our main result is:

**Theorem 4.1.** *Let $p \geq 11$ be a prime number. Let $r \in \mathbb{F}_{p^p}$ be a root of $f(x) = x^p - x - 1$ of order $d = o(r)$. Write $d$ in base $p$ as follows:*

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

*where $0 \leq d_i \leq p-1$. Let $g(p) = \frac{p^p-1}{p-1}$. Assume that*

$$d < g(p).$$

*Then the number $s$ of nonzero $d_i$'s is at least 5, i.e.,*

$$s = \sum_{d_i > 0} 1 \geq 5.$$

*Proof.* Set $\delta = d_0 + \cdots + d_{p-1}$. Observe that $d_0 = 1$ and that Theorem 3.5 gives $\delta \geq 2p - 1$. So, we have $s \geq 3$. If $s = 3$ the same theorem, together with $d_{p-1} = d_{p-2} = 0$, forces $d$ to have the form

$$d = 1 + (p-1)p^k + (p-1)p^l$$

for some integers $1 \leq k < l \leq p - 3$. From $r^d = 1$, i.e., from

$$r(r+k)^{p-1}(r+l)^{p-1} = 1,$$

one gets by multiplication of both sides by $(r+k)(r+l)$ the contradiction

$$r(r+k+1)(r+l+1) = (r+k)(r+l).$$

So, $s \geq 4$.

Assume that $s = 4$. Then $d$ has the form

$$d = 1 + d_k p^k + d_l p^l + d_m p^m$$

for some integers $1 \leq k < l < m \leq p - 3$. From $r^d = 1$, i.e., from

$$r(r+k)^{d_k}(r+l)^{d_l}(r+m)^{d_m} = 1, \tag{13}$$

one gets by multiplication of both sides of (13), by $(r+l)^{p-d_l}(r+m)^{p-d_m}$,

$$r(r+k)^{d_k}(r+l+1)(r+m+1) = (r+m)^{p-d_m}(r+l)^{p-d_l}. \tag{14}$$

But $\delta = 1 + d_k + d_l + d_m \geq 2p - 1$ so:

$$d_k + 3 \geq 2p - (d_m + d_l),$$

and by symmetry:

$$d_l + 3 \geq 2p - (d_k + d_m),$$

and

$$d_m + 3 \geq 2p - (d_k + d_l).$$

So, remembering that the minimal polynomial of $r$ is of degree $p$, we get from (14), and by symmetry:

$$p - 1 \geq d_k \geq p - 3,$$

$$p - 1 \geq d_l \geq p - 3,$$

$$p - 1 \geq d_m \geq p - 3.$$

Now multiply both sides of (13), by $(r+k)^{p-d_k}(r+l)^{p-d_l}(r+m)^{p-d_m}$ to get

$$r(r+k+1)(r+l+1)(r+m+1) = (r+k)^{p-d_k}(r+l)^{p-d_l}(r+m)^{p-d_m}. \tag{15}$$

But

$$(p - d_k) + (p - d_l) + (p - d_m) \leq 9.$$

So, remembering that the minimal polynomial of $r$ is of degree $p \geq 11$, we see that (15) gives a contradiction, so $s > 4$, thereby finishing the proof of the theorem. □

## 5. Some simple computational issues

We report here on some computations done in order to improve our lower and upper bounds for a range of $p's$. Two computer programs written in Maple were runned on a machine with 8 processors with following results:

**Proposition 5.1.** *Let $S_1$ be the set of primes in between* 103 *and* 257 *and let $S_2$ the set of primes in between* 11 *and* 3511. *Let $p$ be a prime number. Let $r \in \mathbb{F}_{p^p}$ be a root of $f(x) = x^p - x - 1$ of order $d = o(r)$. Let $\mu(p)$ and $k$ be defined as in Corollary 3.2. Then*

a) *For $p \in S_2$ one has that either $d = g(p)$ or*

$$\frac{1}{2}\binom{2p}{p} + 8000p \leq d \leq p^{p-2} - (\mu(p)k + 1)p + 1 - 16000p.$$

b) *For $p \in S_1$ one has that either $d = g(p)$ or*

$$d \leq p^{p-2} - (\mu(p)k + 1)p + 1 - 10^6 p.$$

c) *For $p \in S_1$ one has:*

$$\frac{1}{2}\binom{2p}{p} + 10^8 p \leq d.$$

The computer programs used the trivial fact that one has

$$p^p \equiv 1 \pmod{d}.$$

Timings: 141 seconds for left hand side inequality in a), 497 seconds for right hand side inequality in a). While, b) took 1174 seconds and c) took 9916 seconds on the same machine. Advantage of computing $p^p \pmod{d}$ without really computing $p^p$ was used everywhere on the programs.

## References

[1] N. Bourbaki, *Éléments de mathématique. Algèbre. Chapitres 4 á 7*, Lecture Notes in Mathematics, 864. Masson, Paris, 1981.

[2] S. D. Cohen, *Reducibility of sublinear polynomials over a finite field*, Bull. Korean Math. Soc. **22** (1985), no. 1, 53–56.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, With a foreword by P. M. Cohn. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.

[4] W. F. Lunnon, P. A. B. Pleasants, N. M. Stephens, *Arithmetic properties of Bell numbers to a composite modulus. I*, Acta Arith. **35** (1979), no. 1, 1–16.

[5] W. H. Mills, *The degrees of the factors of certain polynomials over finite fields*, Proc. Amer. Math. Soc. **25** (1970), 860–863.

[6] S. Jr. Wagstaff, *Aurifeuillian factorizations and the period of the Bell numbers modulo a prime*, Math. Comp. **65** (1996), no. 213, 383–391.

Mireille Car
Department of Mathematics
University Aix-Marseille III
Avenue Escadrille Normandie-Niemen
13397 Marseille Cedex 20, France
*E-mail address*: mireille.car@univ-cezanne.fr

Luis H. Gallardo
Mathematics
University of Brest
6, Avenue Le Gorgeu
C. S. 93837, 29238 Brest Cedex 3, France
*E-mail address*: Luis.Gallardo@univ-brest.fr

Olivier Rahavandrainy
Mathematics
University of Brest
6, Avenue Le Gorgeu
C. S. 93837, 29238 Brest Cedex 3, France
*E-mail address*: Olivier.Rahavandrainy@univ-brest.fr

Leonid N. Vaserstein
Department of Mathematics
The Pennnsylvania State University
University Park
PA 16802, U.S.A.
*E-mail address*: vstein@math.psu.edu