Applied Mathematics E-Notes, 16(2016), 72-79 © ISSN 1607-2510
Available free at mirror sites of http://www.math.nthu.edu.tw/∼amen/

A Property Of The Period Of A Bell Number Modulo A Prime Number*

Luis Henri Gallardo†

Received 05 November 2015

Abstract

Given a prime number p, put $q := p^p$ so that $\mathbb{F}_q$ is the Artin-Schreier extension of $\mathbb{F}_p$ with minimal polynomial $m_p(x) := x^p - x - 1$. We prove that $d^2 \mid g(p)$ if and only if $\alpha := r^{Q_{p-2}(p)} = 1$ provided that $p^p \equiv 1 - dp \pmod{d^2}$, where $r \in \mathbb{F}_q$ is any root of $m_p(x)$, $g(p) = \frac{q-1}{p-1}$, $d = 2kp + 1$ is the order of r in the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$ and, where $Q_{p-2}(x), S_{p-2}(x)$ are the unique polynomials in $\mathbb{Q}[x]$ such that $\deg(Q_{p-2}(x)) \leq p - 2$ and

$$1 - x^p = (1 - x) \cdot (1 + 2kx) \cdot Q_{p-2}(x) + x^{p-1} S_{p-2}(x).$$

Moreover, under the same condition, we are able to prove, that indeed $g(p)/d \equiv Q_{p-2}(p) \equiv \frac{p}{1-p} \pmod{d}$ so that $d^2 \nmid g(p)$, and that $2d^2 < g(p)$.

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 [11], other definitions, or characterizations, exist (see, e.g. [1], [4, page 371], [15], [17]). Williams [8] 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 $o(r)$ the order of r in the cyclic group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$. 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 $c(p) := 1 + 2p + 3p^2 + \cdots + (p-1)p^{p-2}$.

It is interesting to observe that the minimal period $d := o(r)$ of $B(n) \pmod{p}$ is conjectured, but not proved, (see [2, 5, 11, 14, 15, 16, 17]). to be equal to $g(p)$, where $g(p) := 1 + p + p^2 + \cdots + p^{p-1}$. We know that d is a divisor of $g(p)$ so that $d \leq g(p)$.

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

†Department of Mathematics, Brest University, C. S. 93837, 29238 Brest Cedex 3, France

Clearly, for any k in $0 \leq k < p$, $B(n) \equiv k \pmod{p}$ satisfies $n \leq d$, 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 [6], where it is proved that indeed $n < \frac{1}{2}\binom{2p}{p}$. Moreover, in [7] it is proved that $2^{2.54p} < d$. Both results are non-trivial. In other words one has

$$n < \frac{1}{2}\binom{2p}{p} < 2^{2.54p} < d \leq g(p).$$

Furthermore, (see [14, Lemma 1.1]) $d \equiv 1 \pmod{2p}$ always, and $d \equiv 1 \pmod{4p}$ when $p \equiv 3 \pmod{4}$ since d is a divisor of $g(p)$. A recent paper about Bell numbers modulo a prime number is [13].

The purpose of the present paper is to prove the following three theorems. The following condition on p is important for the proofs.

$$p^p \equiv 1 - dp \pmod{d^2}. \tag{1}$$

Our first theorem consists of observing the following fact about $d = o(r)$ that appears unnoticed. See Lemma 1 for the definition of $Q_{p-2}(p)$.

THEOREM 1. Assume that p satisfies (1). Then d^2 divides $g(p)$ if and only if $\alpha := r^{Q_{p-2}(p)} = 1$.

The second theorem proves that the condition $d^2 \mid g(p)$ in Theorem 1 does not hold.

THEOREM 2. Assume that p satisfies (1). One has that $\frac{g(p)}{d} \equiv \frac{p}{1-p} \pmod{d}$ so that the condition in Theorem 1 does not hold, i.e., $d^2 \nmid g(p)$.

The third theorem gives a non-trivial upper bound for d.

THEOREM 3. Assume that p satisfies (1). If $d < g(p)$ then $2d^2 < g(p)$.

REMARK 1. Sligthly better upper bounds are possible in Theorem 3, with the same method (see proof).

REMARK 2. It is easy to see that the condition $d^2 \mid g(p)$ in Theorem 1 is also equivalent to

(a) $\alpha \in \mathbb{F}_p$ since $N(\alpha) = 1$.

(b) $B(n) \equiv 0 \pmod{p}$ for $n := Q_{p-2}(p) + c(p) + 1$ since this is equivalent to $\mathrm{Tr}(\alpha) = 0$ by definition of period of $B(n)$ and from [9, Theorem 2] (quoted as [13, formula (1)]) and since $\mathrm{Tr}(r^{c(p)}) \neq 0$ (see Lemma 2).

REMARK 3. Although by Theorem 2, d^2 does not divide $g(p)$, provided $p^p \equiv 1 - dp \pmod{d^2}$, it is unknown if $g(p)$ is divisible by a square of a number, for some prime number p. Some numerical evidence obtained over small prime numbers p suggests

that $g(p)$ should be square-free. Since factoring $g(p)$ is non-trivial for large primes p, we may consider the very special case in which $g(p)$ itself is a square. This can be checked (false) quickly even for large primes. But, indeed these computations are not necessary since it follows immediately from Ljunggren's result (see Lemma 3) that for any odd prime number p (and for $p = 2$ directly), $g(p)$ is never the square of an integer. On the other hand, a proof that $g(p)$ is actually square-free, for any prime p, appears hopeless at present.

The following interesting remark on the size of possible squares dividing $g(p)$ is from the referee.

REMARK 4. The *abc* conjecture implies that any square dividing $p^p - 1$ should be relatively small. In particular, the condition $d^2 \mid g(p)$ in Theorem 1 is (a priori) unlikely to hold.

REMARK 5. It is interesting to know whether or not these theorems can hold unconditionally. We explain in Lemma 4 below several equivalent forms of the condition (1).

2 Some Tools

The following lemma follows from considering A/B modulo x^{n+1}.

LEMMA 1. Let p be a prime number, let k be a positive integer, and let n be any nonnegative integer. Let $A := 1 - x^p$ and $B := (1 - x)(1 + 2kx)$. Then there exist unique polynomials with rational coefficients Q_n and S_n such that $\deg(Q_n) \leq n$ and

$$A = BQ_n + x^{n+1}S_n.$$

The following lemma is contained in [13, Lemma 8, Lemma 42].

LEMMA 2. Let $e := Tr(y)$ where y is any nonzero solution of the equation $y^p = ry$ in $\mathbb{F}_q$. We put $a := Tr(r^{c(p)})$ and $b := Tr(r^{-c(p)})$. Then

(i) a and b satisfy $ab \equiv -1 \pmod{p}$, so that they are both nonzero in $\mathbb{F}_p$.

(ii) e is nonzero.

(iii) $a = B(c(p))$ so that $b = \frac{-1}{B(c(p))}$.

The following lemma of Ljunggren [3] is included in [12, Theorem NL].

LEMMA 3. Equation

$$\frac{x^n - 1}{x - 1} = y^2, \text{ in integers } x > 1, y > 1, n > 2,$$

has the unique solution $(x, y, n) = (7, 20, 4)$.

LEMMA 4. Put $d := 2kp + 1$, $b := \frac{(2k)^p+1}{2k+1}$. The following statements are all equivalent

(a) $p^p \equiv 1 - dp \pmod{d^2}$.

(b) $g(p)/d \equiv p/(1-p) \pmod{d}$.

(c) $b \equiv 0 \pmod{d^2}$.

(d) $b_0/d \equiv p^2/(1-p) \pmod{d}$ and $b_1 \equiv p^2/(p-1) \pmod{d}$, where $b = b_0 + b_1 d \pmod{d^2}$.

PROOF. Since $2k = (d-1)/p$ we obtain immediately $b \equiv b_0 + b_1 d \pmod{d^2}$ where

$$b_0 = \frac{p}{p-1}\left(1 - \frac{1}{p^p}\right) \tag{2}$$

and

$$b_1 = \frac{p}{(p-1)^2}\left(\frac{1}{p^p}(p^2 - p) + \frac{1}{p^p} - 1\right). \tag{3}$$

Since $g(p) = \frac{p^p-1}{p-1}$ one sees that (a) is equivalent to (b). One sees that $b_0 \equiv 0 \pmod{d}$ since $p^p \equiv 1 \pmod{d}$. For the same reason we get $b_1 \equiv \frac{p^2}{p-1} \pmod{d}$. We have also $\frac{b_0}{d} = \frac{g(p)}{dp^{p-1}} \equiv \frac{pg(p)}{d} \pmod{d}$. Observe also that $b \equiv 0 \pmod{d^2}$ is equivalent to $\frac{b_0}{d} + b_1 \equiv 0 \pmod{d}$. Finally observe that p and $(p-1)$ are both inversible modulo d and modulo d^2. The result follows.

3 Proof of Theorem 1

If $d = g(p)$ the condition (1) is void so that $d < g(p)$ in what follows. Apply Lemma 1 with $n := p - 2$ to get

$$A := BQ_{p-2} + x^{p-1}S_{p-2}, \tag{4}$$

where A and B are defined as in Lemma 1. Write $Q_{p-2} = Q_{p-2}(x) = q_0 + q_1 x + \cdots + q_{p-2}x^{p-2}$. Observe that the q_s's are integers defined by

$$q_s = \frac{1 - (-2k)^{s+1}}{2k+1}, \text{ for } s = 0, \ldots, p-2, \tag{5}$$

so that, in particular, $q_{p-2} \neq 0$. Since both sides of (4) have the same degree and $\deg(BQ_{p-2}) = 2 + p - 2 = p$ we obtain

$$\deg(x^{p-1}S_{p-2}) \leq p. \tag{6}$$

Thus (6) implies

$$\deg(S_{p-2}) \leq 1.$$

Case 1. $\deg(S_{p-2}) < 1$. In other words, $S_{p-2} = c$ for some constant. Replace $x = 1$ into both sides of (4) to get $c = 0$, i.e., $S_{p-2} = 0$ so that

$$A = BQ_{p-2}. \tag{7}$$

But, (7) implies the contradiction that $-\frac{1}{2k} \neq 1$ is a rational root of the irreducible polynomial $\frac{A}{1-x} = 1 + x + \cdots + x^{p-1}$. Thus Case 1 can't happen.

Case 2. $\deg(S_{p-2}) = 1$, say, $S_{p-2} = ax + b$ with $a \neq 0$. Replace $x = 1$ into both sides of (4) to get $a = -b$, i.e., $S_{p-2} = b(1 - x)$ so that by dividing both sides of (4) by $1 - x$ one gets in $\mathbb{Q}[x]$ (indeed in $\mathbb{Z}[x]$),

$$\frac{1 - x^p}{1 - x} = (1 + 2kx)Q_{p-2}(x) + bx^{p-1}. \tag{8}$$

It follows from (5) that

$$q_{p-2} = \frac{1 - (2k)^{p-1}}{1 + 2k}. \tag{9}$$

On the other side, by computing the leading coefficient in both sides of (8) one gets

$$b = 1 - 2kq_{p-2}. \tag{10}$$

Thus, from (9) and (10) we obtain

$$b = \frac{(2k)^p + 1}{2k + 1}. \tag{11}$$

Choose k such that $d = 2kp + 1$. Thus it follows from (4) that

$$\frac{g(p)}{d} = \frac{A(p)}{B(p)} = Q_{p-2}(p) + \frac{b}{d}p^{p-1}. \tag{12}$$

Set $\alpha := r^{Q_{p-2}(p)}$. Now, by part c) of Lemma 4 we have $b \equiv 0 \pmod{d^2}$, so that we get from (12)

$$Q_{p-2}(p) \equiv \frac{A(p)}{B(p)} \equiv \frac{g(p)}{d} \pmod{d}. \tag{13}$$

Therefore, we see from (13) that d divides $Q_{p-2}(p)$, i.e., $\alpha = 1$, is equivalent to

$$d^2 \mid g(p).$$

thereby proving the claim.

4 Proof of Theorem 2

Follows immediately from part b) of Lemma 4.

5 Proof of Theorem 3

Define f by $g(p) = df$. From (13) and from Lemma 4 we get

$$f \equiv \frac{p}{1-p} \pmod{d}. \tag{14}$$

Thus, for some positive integer M one has

$$f(p-1) + p = Md. \tag{15}$$

Since d and f are divisors of $g(p)$ both are congruent to 1 (mod p). Thus, (15) implies $M = Np - 1 \geq p - 1$, for some positive integer N. But, by (15), M is odd, so that $Md \geq pd$. In other words (15) becomes

$$f(p-1) \geq p(d-1). \tag{16}$$

So by multiplication of both sides of (16) by d, we obtain

$$d(d-1) \leq \frac{p^p - 1}{p} < g(p) = df. \tag{17}$$

Thus, (17) implies $d - 1 < f$. But, d and f are both odd so that $f \geq d$. In other words we get $d^2 \leq g(p)$. But by Lemma 3, (or by Theorem 2), we have indeed $d^2 < g(p)$. Recall that $d \mid g(p)$. Thus, recalling also that d and $g(p)$ are both odd and both equal to 1 modulo p; and that $g(p) \equiv 1 \pmod 4$, one has

$$d^2 = g(p) - 4Kdp. \tag{18}$$

for some positive integer K.

Divide both sides of (18) by dp, reduce modulo d, and use Theorem 2 to get

$$4K \equiv \frac{g(p)}{dp} \equiv \frac{1}{1-p} \pmod{d}. \tag{19}$$

In other words, (19) really says that for some positive integer L one has

$$4K(p-1) + 1 = dL \geq d. \tag{20}$$

From (20) we get successively: $4K \geq \frac{d-1}{p-1} > \frac{d-1}{p}$ so that $4Kp > d - 1$. Thus (18) implies

$$g(p) > d^2 + d(d-1). \tag{21}$$

Now, proceeding as before we see, from (21), that $g(p) = d^2 + d(d-1) + dT$ where the positive integer T satisfies $T \equiv \frac{1}{1-p} \pmod{d}$. Thus $d \mid T(p-1) + 1$ that leads to the inequality $T \geq \frac{d-1}{p-1}$. Observe that $(d-1)(1 + \frac{1}{p-1}) > d$, since $p < d$. Therefore we have

$$g(p) \geq d^2 + d(d-1)\left(1 + \frac{1}{p-1}\right) > d^2 + d^2, \tag{22}$$

thereby completing the proof of Theorem 3.

Acknowledgment. We thank the referee for careful reading, and for great suggestions that lead to an improved paper. In particular the simpler proof of Lemma 1 was suggested by the referee. We do not know how to answer the following two nice questions of the referee: Does $Q_{p-2}(p) \mid g(p)$? and if not, how big does become $\gcd(Q_{p-2}(p), g(p))$?. But these questions are very motivating in order to try to advance further, in the future, on trying to understand the relation between d and $g(p)$.

References

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

[2] L. Carlitz, Congruences for generalized Bell and Stirling numbers, Duke Math. J., 22(1955), 193–205.

[3] W. Ljunggren, Noen Setninger om ubestemte likninger av formen $\frac{x^n-1}{x-1} = y^q$, Norsk. Mat. Tidsskr., 25(1943), 17–20.

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

[5] C. Radoux, Arithmétique des nombres de Bell et analyse modulo p-adique, Bull. Soc. Math. Belg., 29(1977), 13–28.

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

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

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

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

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

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

[12] P. Mihăilescu and Y. Bugeaud, On the Nagell-Ljunggren equation $\frac{x^n-1}{x-1} = y^q$, Math. Scand., 101(2007), 177–183.

[13] O. Rahavandrainy and L. H. Gallardo, Bell numbers modulo a prime number, traces and trinomials, Electron. J. Combin., 21(2014), Paper 4.49, 30pp.

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

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

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

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