Conspectus materiae tomi XXXV, fasciculi 1

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-01224-2 ISSN 0065-1036

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

Arithmetic properties of Bell numbers to a composite modulus I

by

W. F. Lunnon, P. A. B. Pleasants and N. M. Stephens (Cardiff)

1. Introduction. The *Bell numbers* $B(n)$ may be defined in various ways:

(1.1) Definition. Combinatorially: $B(n)$ = the number of partitions of a set of n distinct objects into nonempty subsets.

(1.2) Definition. By Dobinski's formula:

$$B(n) = e^{-1}\sum_{n=0}^{\infty} i^n/i!.$$

(1.3) Definition. By exponential generating function:

$$e^{e^z-1} = \sum_{n=0}^{\infty} B(n)z^n/n!.$$

Their first few values are tabulated at (1.8). The survey article [10] by Rota discusses their elementary properties and has a large bibliography. Several authors ([2], [7], [10], [13]–[15]) have investigated their "arithmetic" behaviour modulo a prime p, establishing the linear recurrence of Touchard (5.4)

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

and the periodicity

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

where

$$l = (p^p-1)/(p-1).$$

Calculations [7] have shown that l is the minimum period for small p; however, its minimality for all p remains undecided.

Carlitz [4] (brought to our attention by the referee) investigated a generalization of $B(n)$ modulo a prime power p^s, establishing our (5.9), (his 6.9), and the upper bound part of our period (6.2), (his 6.8). Touchard also noted some oddments modulo a composite m in [14]. We shall establish in Section 3 that the minimum linear recurrence satisfied by $B(n)$ modulo m has degree r, where r is the smallest number such that $r!$ is divisible by m; and that the coefficients of this recurrence may be taken as the rth row of the matrix $(\boldsymbol{SC})^{-1}$, where $\boldsymbol{S}$ and $\boldsymbol{C}$ are formed in the natural way from Stirling type II numbers and binomial coefficients; and in Section 6 that the period of $B(n)$ modulo p^s divides, with quotient coprime to p,

$$l = p^{s-i}(p^p-1)/(p-1)$$

where

$$i = \begin{cases} 1 & \text{if} \quad p>2 \text{ or } s=1, \\ 0 & \text{if} \quad p=2 \text{ and } s>1. \end{cases}$$

A full period of $B(n)$ modulo various m is displayed at (1.7).

"Umbral" calculus will be employed to render proofs more readable and succinct: B^n is written for $B(n)$, and the resulting polynomials in the operator B are more or less freely manipulated. For instance

$$B^{n+1} = (B+1)^n \tag{1.5}$$

(as in (4.2)) means

$$B(n+1) = \sum_k \binom{n}{k} B(k);$$

Touchard's recurrence (henceforth TR) becomes

$$B^n(B^p-B-1) \equiv 0 \pmod{p}; \tag{TR}$$

in which setting $n \to 0$ yields

$$B^p \equiv 2 \pmod{p}. \tag{1.6}$$

We distinguish three increasingly powerful sorts of umbral relation. "Equations" or "congruences" such as (1.5), (1.6), (4.5) are valid only as they stand. "Recurrences" such as (TR), (5.9), (6.1) have a factor B^n – often implicit – and are valid for arbitrary n. "Identities" such as (4.10) are valid for any transcendental x in place of B. Recurrences modulo m may be added and multiplied just like identities, with one exception: if $h(B) \equiv 0 \pmod{m}$ and $h'(B) \equiv 0 \pmod{m'}$ are recurrences, then $h(B)h'(B) \equiv 0 \pmod{mm'}$ is a recurrence only if at least one of h, h' is an identity. For example, the give-and-take principle (4.8) works even if $f \equiv g$ is only a recurrence, since (4.7) is an identity (of degree zero); on the other hand, from (TR) it does not follow that

$$B^n(B^p-B-1)^2 \equiv 0 \pmod{p^2}.$$

In fact, the correct exponent on the left hand side is 3 – see (5.9).

Within proofs, the factor B^n and the congruence modulus m or p^s may be omitted. A right arrow within the invocation of a theorem denotes substitution: e.g. "(TR) with $p \to 2$" means "$B^n(B^2-B-1) \equiv 0 \pmod{2}$".

Alphabetic conventions: lower case italic letters normally represent natural numbers, except that: $a, b, c, \ldots$ may be integers where this makes sense; f, g, h are polynomials, usually in B; i, j, k are subscripts whose range, if unstated, may be deduced from the context; p is a prime; x, y, z are transcendentals. Boldface upper-case letters represent matrices; lower-case, vectors; B, C umbral operators.

(1.7) TABLE. Residues of $B(n)$ modulo m:

m \ n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	1	1	0	...																
3	1	1	2	2	0	1	2	1	0	0	1	0	1 ...							
4	1	1	2	1	3	0	3	1	0	3	3	2	...							
8	1	1	2	5	7	4	3	5	4	3	7	2	5	5	2	1	3	4	7	1
9	1	1	2	5	6	7	5	4	0	6	1	6	4	1	7	5	5	0	4	5

m \ n	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
8	4	7	3	2	...															
9	1	6	6	1	6	4	1	1	5	2	6	4	5	4	6	3	1	6	1	...

(1.8) TABLE. Values of $B(n)$, $0 \leqslant n \leqslant 15$:

1(0), 1(1), 2(2), 5(3), 15(4), 52(5), 203(6), 877(7), 4140(8), 21147(9), 115975(10), 678570(11), 4213597(12), 27644437(13), 190899322(14), 1382958545(15).

2. Binomial coefficients and Stirling numbers. Here we briefly review some standard combinatorial definitions and results, expounded more fully in (7.9), (7.14).

$$\binom{n}{m} = n!/m!(n-m)! = \binom{n}{n-m} \tag{2.1}$$

denotes the binomial coefficient, with its well-known recursion

$$\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}, \tag{2.2}$$

and the binomial theorem

$$(x+y)^n = \sum_k \binom{n}{k} x^k y^{n-k}. \tag{BT}$$

(2.3) LEMMA. *The number of ways to choose, without repetition, a subset of size m from a set of size n is* $\binom{n}{m}$.

(2.4) LEMMA. *With repetition, the number is* $\binom{n+m-1}{m}$.

Stirling's factorial approximation:

$$n! = \prod_{k=1}^{n} k \sim e^{-n} n^n \sqrt{2\pi n}. \tag{2.5}$$

$S(n, m)$ denotes the type II Stirling number, the number of ways to partition a set of size n into m nonempty subsets. By (1.1)

$$B(n) = \sum_k S(n, k). \tag{2.6}$$

The type I number $s(n, m)$ is defined by matrix inversion,

$$\sum_k S(m, k) s(k, n) = \delta_{mn}. \tag{2.7}$$

Fundamental recursions are

$$\begin{aligned} S(n, m) &= S(n-1, m-1) + mS(n-1, m); \\ s(n, m) &= s(n-1, m-1) - (n-1)s(n-1, m). \end{aligned} \tag{2.8}$$

Arithmetic behaviour modulo p^s is discussed in [2], [4].

We now define some special matrices. The row and column subscripts i and j shall run from 0 to r or ∞. For clarity the initial segments of size 5×5, that is $0 \leqslant i, j \leqslant 4 = r$, are shown at (2.11).

$\boldsymbol{S}$ is defined to be $\|S(i, j)\|$, and its inverse $\boldsymbol{S}^{-1}$ is got from (2.7). $\boldsymbol{C}$ is $\left\|\binom{i}{j}\right\|$, and its inverse is got from

$$\sum_k \binom{m}{k} (-)^{k+n} \binom{k}{n} = \delta_{mn}, \tag{2.9}$$

proved by considering the coefficient of x^n in $\big((x-1)+1\big)^m$. $\boldsymbol{B}$ is $\|B(i+j)\|$, and $\boldsymbol{F}$ is the diagonal of factorials $\|j!\,\delta_{ij}\|$. Finally $\boldsymbol{D} = \boldsymbol{SC}$; explicitly, $\boldsymbol{D} = \|d_{ij}\|$ and $\boldsymbol{D}^{-1} = \|e_{ij}\|$ where

$$d_{ij} = \sum_k S(i, k)\binom{k}{j}, \qquad e_{ij} = \sum_k (-)^{i+k}\binom{i}{k} s(k, j). \tag{2.10}$$

$$\begin{array}{ccccc} 1 & 1 & 2 & 5 & 15 \\ 1 & 2 & 5 & 15 & 52 \\ 2 & 5 & 15 & 52 & 203 \\ 5 & 15 & 52 & 203 & 877 \\ 15 & 52 & 203 & 877 & 4140 \end{array} \qquad \begin{array}{ccccc} 1 & & & & \\ & 1 & & & \\ & & 2 & & \\ & & & 6 & \\ & & & & 24 \end{array} \tag{2.11}$$

$$\boldsymbol{B} = \|B(i+j)\| \qquad \boldsymbol{F} = \|j!\,\delta_{ij}\|$$

$$\begin{array}{ccccc} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{array} \qquad \begin{array}{ccccc} 1 & & & & \\ -1 & 1 & & & \\ 1 & -2 & 1 & & \\ -1 & 3 & -3 & 1 & \\ 1 & -4 & 6 & -4 & 1 \end{array}$$

$$\boldsymbol{C} = \left\|\binom{i}{j}\right\| \qquad \boldsymbol{C}^{-1} = \left\|(-)^{i+j}\binom{i}{j}\right\|$$

$$\begin{array}{ccccc} 1 & & & & \\ 0 & 1 & & & \\ 0 & 1 & 1 & & \\ 0 & 1 & 3 & 1 & \\ 0 & 1 & 7 & 6 & 1 \end{array} \qquad \begin{array}{ccccc} 1 & & & & \\ 0 & 1 & & & \\ 0 & -1 & 1 & & \\ 0 & 2 & -3 & 1 & \\ 0 & -6 & 11 & -6 & 1 \end{array}$$

$$\boldsymbol{S} = \|S(i, j)\| \qquad \boldsymbol{S}^{-1} = \|s(i, j)\|$$

$$\begin{array}{ccccc} 1 & & & & \\ 1 & 1 & & & \\ 2 & 3 & 1 & & \\ 5 & 10 & 6 & 1 & \\ 15 & 37 & 31 & 10 & 1 \end{array} \qquad \begin{array}{ccccc} 1 & & & & \\ -1 & 1 & & & \\ 1 & -3 & 1 & & \\ -1 & 8 & -6 & 1 & \\ 1 & -24 & 29 & -10 & 1 \end{array}$$

$$\boldsymbol{D} = \|d_{ij}\| = \boldsymbol{SC} \qquad \boldsymbol{D}^{-1} = \|e_{ij}\| = \boldsymbol{C}^{-1}\boldsymbol{S}^{-1}$$

3. Minimal recurrences for $B(n)$. A linear recurrence for $B(n)$ modulo m is a vector $\boldsymbol{a} = (a_j)$ such that, for all n,

$$\sum_j a_j B(n+j) \equiv 0 \pmod{m}; \tag{3.1}$$

or in the matrix notation of Section 2,

$$\boldsymbol{aB} \equiv \boldsymbol{0} \pmod{m}. \tag{3.2}$$

Alternatively, we may regard it as an umbral polynomial

$$f(B) = \sum a_j B^j$$

such that, for all n,

$$B^n f(B) \equiv 0 \pmod{m}.$$

Improper solutions, i.e. multiples of recurrences modulo some proper divisor of m, are excluded by insisting that the a_j have HCF coprime to m. In this section, $\boldsymbol{a}$ and $\boldsymbol{b}$ are $1\times(r+1)$ and $\boldsymbol{B}$ and $\boldsymbol{F}$ are $(r+1)\times\infty$.

(3.3) THEOREM. *Let $r = r(m)$ be the least r for which m divides $r!$. Then $\boldsymbol{a}$ = row r of $\boldsymbol{D}^{-1}$ is a proper solution of* (3.2) *of minimal degree: that is, $a_j = e_{rj}$ is a recurrence fulfilling* (3.1) *(see definition* (2.10)).

Proof by Gaussian elimination on (3.2), employing (3.6): since the transpose $\boldsymbol{D}'$ has integer coefficients and determinant unity, (3.2) is equivalent to

$$\boldsymbol{a}\boldsymbol{B}\boldsymbol{D}'^{-1} \equiv \boldsymbol{0}\boldsymbol{D}'^{-1} = \boldsymbol{0},$$

or to

$$\boldsymbol{a}\boldsymbol{D}\boldsymbol{F} \equiv \boldsymbol{0} \quad \text{by (3.6)},$$

or to

$$\boldsymbol{b}\boldsymbol{F} \equiv \boldsymbol{0} \quad \text{where} \quad \boldsymbol{b} = \boldsymbol{a}\boldsymbol{D};$$

that is, $j!\,b_j \equiv 0 \pmod m$ for all j. Evidently there is no proper solution $\boldsymbol{b}$ unless m divides $r!$; when $b_j = \delta_{jr}$ is a proper solution, and correspondingly $\boldsymbol{a} = \boldsymbol{b}\boldsymbol{D}^{-1}$ = row r of $\boldsymbol{D}^{-1}$. ∎

By examining all possible solutions $\boldsymbol{b}$ in this proof, we see further that

(3.4) COROLLARY. *A polynomial basis for the set of all recurrences satisfying* (3.1) *is the set*

$$\Big(\sum_j e_{ij}B^j \times m/\mathrm{HCF}(m, i!)\Big) \quad \textit{where} \quad i = 0(1)r.$$

So the minimal recurrence is not unique, even to within a constant factor, unless $m = p$ is prime.

(3.5) EXAMPLES of minimal recurrences:

$B^n(1-3B+B^2) \equiv 0 \pmod 2$, by row 2 of $\boldsymbol{D}^{-1}$;

$B^n(1-24B+29B^2-10B^3+B^4) \equiv 0 \pmod 4$ and $\pmod 8$, by row 4;

$B^n(B^4+B^2-1) \equiv 0 \pmod 4$, by adding $2(B+1)B^n(B^2-3B+1)$.

To complete the proof of (3.3) it remains to show that we can diagonalise $\boldsymbol{B}$.

(3.6) THEOREM. $\boldsymbol{B} = \boldsymbol{D}\boldsymbol{F}\boldsymbol{D}'$, *that is,*

$$B(i+j) = \sum_k k!\,d_{ik}d_{jk}. \tag{3.7}$$

Proof. Notice that $d_{ij} = 0$ for $j < 0$ or $j > i$. If $i > 0$,

$$\begin{aligned} d_{ij} &= \sum_k S(i,k)\binom{k}{j} \quad \text{by (2.10)};\\ &= \sum_k \binom{k}{j} S(i-1,k-1) + \sum_k k\binom{k}{j} S(i-1,k) \quad \text{by (2.8)};\\ &= \sum_k \binom{k-1}{j} S(i-1,k-1) + \sum_k \binom{k-1}{j-1} S(i-1,k-1) +\\ &\quad + j\sum_k \binom{k}{j} S(i-1,k) + (j+1)\sum_k \binom{k}{j+1} S(i-1,k) \quad \text{by (2.1), (2.2)};\\ &= d_{i-1,j} + d_{i-1,j-1} + jd_{i-1,j} + (j+1)d_{i-1,j+1} \quad \text{by (2.10)}; \end{aligned}$$

that is, for $i > 0$,

$$d_{ij} = d_{i-1,j-1} + (j+1)(d_{i-1,j} + d_{i-1,j+1}). \tag{3.8}$$

Now temporarily write b_{ij} for the right hand side of (3.7). Then

$$\begin{aligned} b_{i,j+1} &= \sum_k k!\,d_{ik}d_{j+1,k} = \sum_k k!\,d_{ik}\big(d_{j,k-1} + (k+1)d_{jk} + (k+1)d_{j,k+1}\big) \quad \text{by (3.8)};\\ &= \sum_k k!\,d_{ik}\,d_{j,k-1} + \sum_k (k+1)!\,d_{ik}d_{jk} + \sum_k k!\,d_{jk}\,d_{i,k-1}\\ &\qquad\qquad \text{setting } k \to k-1 \text{ in the last term};\\ &= b_{i+1,j} \quad \text{since the previous expression is symmetric in } i \text{ and } j. \end{aligned}$$

So $b_{i,n-i}$ is independent of i; and setting $n = i+j$,

$$\begin{aligned} b_{ij} &= b_{i+j,0} = d_{i+j,0} \quad \text{by definition of } b_{ij};\\ &= \sum_k S(i+j,k) \quad \text{by (2.10) with } i \to i+j,\ j \to 0;\\ &= B(i+j) \quad \text{by (2.6).} \ ∎ \end{aligned}$$

Similarly may be shown

$$e_{ij} = e_{i-1,j-1} - ie_{i-1,j} - (i-1)e_{i-2,j} \tag{3.9}$$

which is useful for tabulating $\boldsymbol{D}^{-1}$.

Finally, from (3.6) can be extracted the curiosity

(3.10) COROLLARY. $|\boldsymbol{B}| = |\boldsymbol{F}| = \prod_{k=0}^{r} k!$, *where $\boldsymbol{B}$ is now $(r+1)\times(r+1)$.*

Proof. $|\boldsymbol{D}| = 1$.

4. Properties of $B(n)$; congruence lemmata. From now on we take the modulus to be a prime power, $m = p^s$. Nothing is thereby lost, since if

$$m = \prod_k m_k$$

is the factorisation of m into powers m_k of distinct primes, then $B(n)(\mathrm{mod}\, m)$ is determined from the set of $B(n)(\mathrm{mod}\, m_k)$ and *vice versa*, *via* the Chinese remainder theorem ([6], Theorem 121):

(4.1) $$B(n)(\mathrm{mod}\, m) = \sum_k \big(B(n)(\mathrm{mod}\, m_k)\big)(m/m_k)\big((m/m_k)^{-1}(\mathrm{mod}\, m_k)\big).$$

And the period $(\mathrm{mod}\, m)$ is the LCM of the periods $(\mathrm{mod}\, m_k)$.

We require the following elementary properties of $B(n)$, expounded more fully in any of [10], [13]–[15]

(4.2) $$B^{n+1} = (B+1)^n$$

which follows from the definition (1.1), by classifying the partitions according to the subset containing the $(n+1)$-th element. Hence for a polynomial $f(B)$,

(4.3) $$Bf(B) = f(B+1).$$

Replacing $f(B)$ by $(B-1)(B-2)\ldots(B-k+1)f(B)$,

(4.4) $$f(B)\prod_{i=0}^{k-1}(B-i) = f(B+k);$$

whence, setting $f(B)\to 1$,

(4.5) $$\prod_{i=0}^{k-1}(B-i) = 1.$$

Also, setting $f(B)\to(B-1)^n$ in (4.3) gives the handy computational formula (where Δ is the forward difference operator)

(4.6) $$B^n = B(B-1)^n = \Delta^n(B).$$

We also require the following congruence properties.

(4.7) Lemma. $\binom{up^s}{vp^t} \equiv 0(\mathrm{mod}\, p^{s-t})$ *if* $v \not\equiv 0(\mathrm{mod}\, p)$.

Shown by counting powers of p in (2.1). There is a quantity of similar results in [12].

(4.8) Lemma. *The "give-and-take" principle: if* $f(x)$, $g(x)$, $h(x)$ *are functions such that, for all* n, t *such that* $r \leqslant t \leqslant s$,

$$x^n f^{p^{t-r}} \equiv x^n g^{p^{t-r}} \ (\mathrm{mod}\, p^t),$$

umbrally, then

$$x^n(f+h)^{p^{s-r}} \equiv x^n(g+h)^{p^{s-r}} (\mathrm{mod}\, p^s).$$

Proof by (BT) and (4.7) with $s\to s-r$, $t\to t-r$, noting that $x^n f^{vp^{t-r}}$ is essentially a power of $x^n f^{p^{t-r}}$. ∎

(4.9) Lemma. $(a+bp)^{up^{s-1}} \equiv a^{up^{s-1}}(\mathrm{mod}\, p^s)$.

Proof by (4.8) noting that $p^{t-1} \geqslant t$. ∎

An identity of Lagrange ([6], Theorem 112):

(4.10) Lemma. $\prod_{k=0}^{p-1}(x-k) \equiv x^p - x(\mathrm{mod}\, p)$.

(4.11) Lemma. *If for all* n $B^n f(B) \equiv 0(\mathrm{mod}\, m)$ *then for any* k *and all* n

$$B^n f(B+k) \equiv 0(\mathrm{mod}\, m).$$

Proof.

$$B^n f(B+k) = \prod_{i=0}^{k-1}(B-i)\cdot(B-k)^n f(B) \text{ by (4.4);}$$

$$\equiv 0 \text{ since } f \text{ is a recurrence. ∎}$$

5. Some extensions of Touchard's recurrence. These comprise explicit formulae (5.5) for minimal recurrences equivalent to those of Section 3, and bounds on the exponents v and u such that $(B^p-B-1)^v \equiv 0$ (5.9), and $B^{pu} \equiv (B+1)^u$ (5.10). For brevity we shall set $C = B^p-B-1$.

The divided difference operator Δ is defined, for given prime p and polynomial $f(B)$, by

(5.1) $$\Delta f = \big(f(B+p)-f(B)\big)/p.$$

By Taylor's theorem, if f has integer coefficients then so has Δf. Easily,

(5.2) Lemma. $\Delta fg = f(B+p)\Delta g + g\Delta f$.

Given any recurrence for B modulo p^{s-1}, we can bootstrap ourselves up to p^s thus:

(5.3) Lemma. *If* $B^n f \equiv 0(\mathrm{mod}\, p^{s-1})$ *then*

$$B^n(C-p\Delta)f \equiv 0(\mathrm{mod}\, p^s).$$

Proof.

$$B^n Cf(B) \equiv B^n\Big(\prod_{k=0}^{p-1}(B-k)-1\Big)f(B) \text{ by (4.10);}$$
$$= (B+p)^n f(B+p) - B^n f(B) \text{ by (4.4);}$$
$$\equiv B^n p\Delta f \text{ by (BT), (5.1), and noticing that}$$
$$f(B+p) \equiv 0(\mathrm{mod}\, p^{s-1}) \text{ by (4.11) with } m\to p^{s-1},\ k\to p. ∎$$

(5.4) Corollary (Touchard's recurrence).

$C \equiv 0(\mathrm{mod}\, p)$ *by* (5.3) *with* $s\to 1$, $f\to 1$.

With the aid of (5.3) the following recurrences $g_s(B) \equiv 0 \pmod{p^s}$ may be constructed. By (3.3) they are minimal when $p \geqslant s$; but they are not identical to the rows of D^{-1}.

$$(5.5)\qquad \begin{aligned} g_0 &= 1, \\ g_1 &= C, \\ g_2 &= C^2+p, \\ g_3 &= C^3+3pC-p^2, \\ g_4 &= C^4+6pC^2-4p^2C+p^2(p+3), \\ g_5 &= C^5+10pC^3-10p^2C^2+5p^2(p+3)C-p^3(p+10). \end{aligned}$$

Recurrences which are powers of C are most easily investigated *via* a more general expression. Let h_r temporarily denote an arbitrary polynomial of the form

$$(5.6)\qquad h_r = \prod_{i=1}^{r} (C+pf_i)$$

where the f_i are arbitrary polynomials in B.

(5.7) Lemma. *Given r and s, if*

$$B^n h_{r-1} \equiv 0 \pmod{p^{s-1}} \quad \textit{for all } h_{r-1},$$

then

$$B^n h_r \equiv B^n C^r \pmod{p^s} \quad \textit{for all } h_r.$$

Proof by induction on r: for any h_r there is an h_{r-1} such that

$$h_r = (C+pf_r)h_{r-1}.$$

So $h_r - Ch_{r-1} = pf_r h_{r-1} \equiv 0$ by assumption; that is, $h_r \equiv Ch_{r-1}$. We can similarly eliminate the rest of the f_i, so $h_r \equiv C^r$. ■

(5.8) Lemma. $B^n h_{2s-1} \equiv 0 \pmod{p^s}$ *for all* h_{2s-1}.

Proof by induction on s: let $r = 2s-1$, and suppose $h_{r-2} \equiv 0 \pmod{p^{s-1}}$; then $h_{r-1} \equiv 0 \pmod{p^{s-1}}$, being a multiple of h_{r-2}. Now

$$\begin{aligned} h_r &\equiv C^r \pmod{p^s} \quad \text{by (5.7)}; \\ &\equiv p\Delta C^{r-1} \quad \text{by (5.3) with } f \to C^{r-1}; \\ &= p\Delta C \times \sum_{i=0}^{r-2} C^{r-2-i} C(B+p)^i, \end{aligned}$$

where $C(B+p)$ means $(B+p)^p - (B+p) - 1$, by repeated application of (5.2);

$$= p\Delta C \times \sum_i h_{r-2} \equiv 0 \text{ by (5.8) with } s \to s-1.$$

For $s \to 1$, the result is immediate by (TR). ■

(5.9) Theorem. $B^n C^{2s-1} \equiv 0 \pmod{p^s}$ *by* (5.8).

These results are not optimal: for instance, if $2s-3 \geqslant p > 3$ they may be sharpened — see [8] — to

$$h_{2s-2} \equiv 0 \quad \text{and} \quad C^{2s-3} \equiv 0.$$

Finally, a congruence which is a power of C split between right and left sides:

(5.10) Theorem. *If p is an odd prime,*

$$B^n B^{p^s} \equiv B^n (B+1)^{p^{s-1}} \pmod{p^s} \ \textit{exactly};$$

that is, modulo p^{s+1} there is some n for which the recurrence fails.

Proof by induction on s: we first restate (5.10) in the stronger form

$$(5.11)\qquad (B+1)^{p^{s-1}} = B^{p^s} - C^{p^{s-1}} + pg(B),$$

where $g \equiv 0 \pmod{p^{s-1}}$ exactly. This is sufficient by (5.9) with $s \to s+1$, if $p^{s-1} \geqslant 2s+1$, that is

$$(5.12)\qquad p \geqslant 5 \text{ and } s \geqslant 2, \quad \text{or} \quad p=3 \text{ and } s \geqslant 3.$$

For $s > 2$,

$(B+1)^{p^{s-1}} = \left((B+1)^{p^{s-2}}\right)^p = (B^{p^{s-1}} - C^{p^{s-2}} + pf)^p$ by (5.11) with $s \to s-1$,
where $f \equiv 0 \pmod{p^{s-2}}$ exactly;

$$= (B^{p^{s-1}} - C^{p^{s-2}})^p + p^2(B^{p^{s-1}} - C^{p^{s-2}})^{p-1} f + ph$$

by (BT), where $h \equiv 0 \pmod{p^s}$ since it is a multiple of $p^2 f$;

$$= B^{p^s} - C^{p^{s-1}} + p^2 B^{p^{s-1}(p-1)} f + ph$$

by (BT) and (5.9): the other terms, all multiples of $pC^{p^{s-2}}$, may be absorbed into ph provided $p^{s-2} \geqslant 2s-1$, that is

$$(5.13)\qquad p \geqslant 5 \text{ and } s \geqslant 3, \quad \text{or} \quad p = 3 \text{ and } s \geqslant 4.$$

Now set

$$g = pB^{p^{s-1}(p-1)} f + h;$$

since $f \equiv 0 \pmod{p^{s-2}}$ exactly and $h \equiv 0 \pmod{p^s}$, $g \equiv 0 \pmod{p^{s-1}}$ exactly. This is the inductive step.

It remains to treat the initial cases excluded by (5.12), (5.13). For (5.11) with $s = 2$, by definition of C,

$$(B+1)^p = (B^p - C)^p = B^{p^2} - C^p + pg \text{ by (BT)},$$

where $g = B^{p(p-2)}[-B^pC+\frac{1}{2}(p-1)C^2]+C^3f$. Since $C^3 \equiv 0 \pmod{p^2}$ by (5.9), we have to show that the expression [ ] is zero $\pmod{p}$ exactly. The method involves a basis (3.4) for the recurrences modulo p^2 and p in turn. If $s \leqslant p$ (5.5) gives the convenient basis $(g_i p^{s-i})$, $i = 0(1)s$. Reducing the expression modulo these bases should yield non-zero and zero residues respectively. In this case the bases are

$$(p^2,\ pC,\ C^2+p) \quad \text{and} \quad (p,\ C);$$

and the residues of the expression are

$$\begin{aligned} -(B+1)C-\tfrac{1}{2}p(p-3) &\not\equiv 0 \pmod{p^2} \text{ by (3.3)},\\ &\equiv 0 \pmod{p}. \end{aligned}$$

Similarly, omitting computational details, for (5.11) with $s = 3$ and $p = 3$,

$$(B+1)^9 = B^{27}-C^9+pg;$$

with residues

$$\begin{aligned} B^{-18}g &\equiv -pC(B+1)^2+p^2B \pmod{p^3},\\ &\equiv 0 \pmod{p^2}. \end{aligned}$$

For (5.10) with $s = 2$ and $p = 3$, the residues of

$$(B+1)^3-B^9$$

turn out the same as for $B^{-18}g$ above.

For (5.10) with $s = 1$, use (TR) and (3.3). ■

6. The periodicity of $B(n)$. Firstly, let p be an odd prime. Continuing on from (5.10) we shall establish a binomial recurrence (6.2) giving a period of $B(n)$.

(6.1) LEMMA. $B^nB^{p^{s-1+t}} \equiv B^n(B+t)^{p^{s-1}} \pmod{p^s}$, *$p$ odd.*

Proof by induction on t: trivial for $t \to 0$. For $t > 0$,

$$\begin{aligned} 0 &\equiv (C^{p^{t-1}})^{p^{s-1}} \text{ by (5.9), since } p^{s-1} \geqslant 2s-1;\\ &\equiv (B^{p^t}-B^{p^{t-1}}-1)^{p^{s-1}} \text{ by (BT), (4.9)};\\ &\equiv (B^{p^t}-B-t)^{p^{s-1}} \text{ by (6.1) with } t \to t-1, \text{ (4.8) with}\\ &\qquad h \to B^{p^t}-1,\ f \to -B^{p^{t-1}},\ g \to -(B+t-1),\ r \to 1; \end{aligned}$$

so (6.1) holds by (4.8), with $r \to 1$, $f \to B^{p^t}-B-t$, $g \to 0$, $h \to B+t$. ■

(6.2) THEOREM. *For odd p let $l = l(p^s) = p^{s-1}(p^p-1)/(p-1)$. Then*

$$B^{n+l} \equiv B^n \pmod{p^s} \quad \text{for all } n;$$
$$B^{n+l/p} \not\equiv B^n \pmod{p^s} \quad \text{for some } n \ (s \geqslant 2).$$

Proof. Notice that, for $s \geqslant 2$,

$$\begin{aligned} B^{l/p-p^{s-2}}(B-1)^{p^{s-1}} &\equiv B^{l/p-p^{s-2}}(B+p-1)^{p^{s-1}} \text{ by (4.9)};\\ &\equiv B^{p^{s-1}+\dots+p^{s+p-2}} \text{ by (6.1) with } t \to p-1;\\ &\equiv \prod_{k=0}^{p-1}(B+k)^{p^{s-1}} \text{ by (6.1) with } t \to k;\\ &\equiv (B^p-B)^{p^{s-1}} \text{ by (4.10), (4.9)};\\ &\equiv 1 \text{ by (4.8) with } r \to 1,\ f \to C,\ g \to 0,\ h \to 1, \text{ and (5.9)} \end{aligned}$$

noticing that $2t-1 \leqslant p^{t-1}$.

It follows that $B^{l/p} \equiv 1$ is equivalent to

$$(B-1)^{p^{s-1}} \equiv B^{p^{s-2}},$$

or

$$B^{p^{s-1}} \equiv (B+1)^{p^{s-2}} \text{ by (4.11) with } k \to 1.$$

This last is false modulo p^s but true modulo p^{s-1}, by (5.10). ■

(6.3) COROLLARY. $\sum_{k=0}^{l-1} B(n+k) \equiv 0 \pmod{p^s}$, $l = l(p^s)$.

Proof. Evidently

$$\begin{aligned} \sum_k B(n+k) &= \sum_k B(n+1+k)-(B(n+l)-B(n))\\ &\equiv c, \text{ a constant by (6.2).} \end{aligned}$$

Then for any polynomial $f(B)$

$$\sum_k B^k f(B) \equiv c \cdot f(1);$$

choosing $f(B) \to C^{2s-1}$, $f(1) \to (-1)^{2s-1} = -1$,

$$-c \equiv \sum_k B^k C^{2s-1} \equiv 0 \text{ by (5.9).} \ ■$$

Secondly, let $p = 2$.

(6.4) THEOREM. *Let $l = l(2^s) = 3 \cdot 2^s$ for $s \geqslant 2$; 3 for $s = 1$. Then*

$$B^{n+l} \equiv B^n \pmod{2^s},$$

and l is minimal.

Proof. For $s \geqslant 2$,

$$\begin{aligned} B^{l/2} &= (B^3)^{2^{s-1}}\\ &= (1+(B+1)C+2B)^{2^{s-1}} \equiv (1+(B+1)C)^{2^{s-1}} \text{ by (4.9)};\\ &\equiv 1+\binom{2^{s-1}}{2}(B+1)^2C^2+\binom{2^{s-1}}{4}(B+1)^4C^4 \text{ by (BT), (4.7), (5.9)}; \end{aligned}$$

that is,

$$B^{l/2}-1 \equiv 2^{s-3}(2^{s-1}-1)g$$

where we now have to examine the recurrence status of

$$g = 2(B+1)^2C^2+\tfrac{1}{3}(2^{s-2}-1)(2^{s-1}-3)(B+1)^4C^4$$

modulo 2^2 and 2^3. Suppose $s \geqslant 5$; then

$$g \equiv 2(B+1)^2C^2+(B+1)^4C^4 \pmod{2^3}.$$

Then, as in the proof of (5.10), we reduce modulo the sets (5.5) (which suffice; even though in principle we might need the minimal recurrences (3.4))

$$(8,\ 4C,\ 2C^2+4,\ C^3+6C-4)$$
$$(4,\ 2C,\ C^2+2)$$

to get residues

$$g \equiv 4 \pmod{2^3} \equiv 0 \pmod{2^2}.$$

So $B^{l/2} \equiv 1 \pmod{p^{s-1}}$ but not $\pmod{p^s}$, $s \geqslant 5$. For $s = 2, 3, 4$ the argument can be modified, or brute force used (1.7) since the period cannot exceed $l(2^s)$. For $s = 1$ the period is actually 3 (1.7), so no divisor of l is redundant and (6.4) is proved. ■

(6.5) COROLLARY. $\sum_{k=0}^{l-1} B(n+k) \equiv 0 \pmod{2^s}$.

Proof. As in (6.3). ■

We have shown (6.2)–(6.4) that $l(p^s)/p$ is never a period of $B(n)$ $\pmod{p^s}$. Evidently the true period modulo p divides that modulo p^s; so to complete the proof of the minimality of $l(p^s)$ we should have to show that no proper factor of $l(p)$ is a period modulo p. This has been verified for $p \leqslant 17$ in [7], but remains unsolved in general. We do, however, have a lower bound:

(6.6) THEOREM. *The period of $B(n) \pmod{p}$ is at least*

$$\tfrac{1}{2}\binom{2p}{p} \sim 4^p(4\pi p)^{-1/2}.$$

Proof. Consider the set of polynomials

$$B^{\left(n+\sum_{i=0}^{p-1} k_i p^i\right)} \equiv B^n \prod_{i=0}^{p-1} (B+i)^{k_i} \pmod{p} \tag{6.7}$$

by (6.1) with $s \to 1$; where the sequences (k_i) satisfy

$$\sum_{i=0}^{p} k_i = p-1 \quad \text{and} \quad 0 \leqslant k_i < p. \tag{6.8}$$

Observe that k_p appears in (6.8) but not in (6.7). Looking at the right hand side of (6.7), no two of these polynomials can be congruent to each other as recurrences for all n: if they were, their difference would yield a recurrence of degree $< p$, contradicting (3.3). So looking at the left hand side of (6.7), among the powers of B there are at least as many incongruent as there are sequences (k_i) satisfying (6.8). Each sequence corresponds to a choice with repetition of $p-1$ values for i from among the $p+1$ numbers $(0, \ldots, p)$, where k_i specifies how often symbol i is chosen, so by (2.4) their number is

$$\binom{2p-1}{p-1} = \tfrac{1}{2}\binom{2p}{p} \quad \text{by (2.1)}.$$

The 4^p estimate follows from (2.1), (2.5). ■

The 4^p of (6.6) compares poorly with the p^p of (6.2). The method appears to be capable of refinement, but only with some difficulty [8].

Finally, it is worth mentioning that the question of the minimality of the period is equivalent to a problem in the theory of finite fields; to determine whether $l(p)$ is the order of x in F_{p^p}, where $x^p - x - 1 = 0$ — see [1] for the background. (6.6) gives a lower bound on this order.

References

[1] A. A. Albert, *Fundamental concepts of higher algebra*, University of Chicago, 1956.

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

[3] G. Birkhoff and S. Maclane, *A survey of modern algebra*, Macmillan, 1953.

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

[5] W. Feller, *An introduction to probability theory and its applications*, vol. 1, chap. 2, Wiley, 1962.

[6] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fourth ed., Clarendon, 1960.

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

[8] W. F. Lunnon and P. A. B. Pleasants, *Arithmetic properties of Bell numbers to a composite modulus II*, to appear.

[9] J. Riordan, *Combinatorial identities*, Wiley, 1968.

[10] G. C. Rota, *The number of partitions of a set*, Amer. Math. Monthly 71 (1964), pp. 498–504.

[11] E. S. Selmer, *Linear recurrence relations over finite fields*, University of Bergen, 1966.
[12] D. Singmaster, *Divisibility of binomial coefficients by primes and prime powers*, available from the author, Polytechnic of the South Bank, London 1974.
[13] J. Touchard, *Proprietes arithmetiques de certains nombres recurrents*, Ann. Soc. Sci. Bruxelles 53A (1933), pp. 21–31.
[14] — *Nombres exponentiels et nombres de Bernoulli*, Canad. J. Math. 8 (1956), pp. 305–320.
[15] G. T. Williams, *Numbers generated by the function e^{e^x-1}*, Amer. Math. Monthly 52 (1945), pp. 323–327.

Received on 4. 3. 1975
and in revised form on 3. 12. 1976 (685)

ACTA ARITHMETICA
XXXV (1979)

Gauss sums and solutions to simultaneous equations over GF(2^y)

by

John D. Fulton (Clemson, S.C.)

1. Introduction. Let $q = 2^y$, $y \geqslant 1$, and let $F = \mathrm{GF}(q)$, the finite field of order q. For $a \in F$, $t(a) = a + a^2 + \ldots + a^{2^{y-1}}$ defines a homomorphism t of the additive group $(F, +)$ onto the additive group of the prime subfield $\{0, 1\}$ of F, and $e(a) = e^{2\pi i t(a)}$ defines a homomorphism e of $(F, +)$ onto the multiplicative group of integers $\{1, -1\}$([3], p. 29).

Thus, it can be seen that

$$\sum_x e(ax) = \begin{cases} q, & a = 0, \\ 0, & a \neq 0. \end{cases} \tag{1.1}$$

Let $F^{1\times s}$ denote the vector space over F consisting of vectors $\chi = (x_1, x_2, \ldots, x_s)$. Let Q be a quadratic form of full rank s on $F^{1\times s}$ and let g be its associated bilinear form. Then there exists a basis for $F^{1\times s}$ ([3], p. 197) such that if $\chi = (x_1, x_2, \ldots, x_s) \in F^{1\times s}$, then $Q(\chi)$ equals precisely one of the following

$$x_1x_{k+1} + x_2x_{k+2} + \ldots + x_kx_{2k} + x_{2k+1}^2, \qquad s = 2k+1, \tag{1.2}$$

$$x_1x_{k+1} + x_2x_{k+2} + \ldots + x_kx_{2k}, \qquad s = 2k, \tag{1.3}$$

$$x_1x_{k+1} + x_2x_{k+2} + \ldots + x_kx_{2k} + x_{2k+1}^2 + x_{2k+1}x_{2k+2} + \beta x_{2k+2}^2, \qquad s = 2k+2, \tag{1.4}$$

where in (1.4), β is any element of F such that the polynomial $u^2 + uv + \beta v^2$ is irreducible in the polynomial ring $F[u, v]$.

We say that quadratic form Q has type $\tau = 0, 1$, or -1 according as Q is equivalent under change of basis for $F^{1\times s}$ to (1.2), (1.3), or (1.4), respectively.