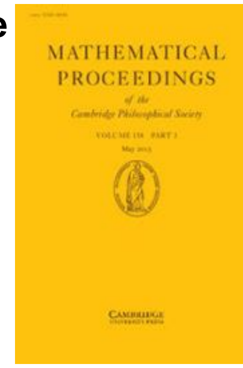

Congruence properties of the binary partition function

R. F. Churchhouse

Mathematical Proceedings of the Cambridge Philosophical Society / Volume 66 / Issue 02 / September 1969, pp 371 - 376
DOI: 10.1017/S0305004100045072, Published online: 24 October 2008

Proc. Camb. Phil. Soc. (1969), **66**, 371
PCPS 66–44
Printed in Great Britain

Congruence properties of the binary partition function

By R. F. CHURCHHOUSE
Atlas Computer Laboratory, Chilton, Didcot, Berks.

(*Received* 4 *October* 1968)

1. *Introduction.* We denote by $b(n)$ the number of ways of expressing the positive integer n as the sum of powers of 2 and we call $b(n)$ 'the binary partition function'. This function has been studied by Euler (1), Tanturri (2–4), Mahler (5), de Bruijn (6) and Pennington (7). Euler and Tanturri were primarily concerned with deriving formulae for the precise calculation of $b(n)$, whereas Mahler deduced an asymptotic formula for $\log b(n)$ from his analysis of the functions satisfying a certain class of functional equations. De Bruijn and Pennington extended Mahler's work and obtained more precise results.

Some time ago I used the Atlas Computer to generate the coefficients of various power series including

$$F(x) = \sum_{n=0}^{\infty} b(n)\, x^n.$$

After studying $b(n)$ I proved that

$$(1) \quad b(n) = O(n^{\frac{1}{2}\log_2 n}) \quad \text{and} \quad (2) \quad b(4n) \equiv b(n) \pmod{2^k},$$

where k is a number which is related to the highest power of 2 which divides n. I was at this time unaware of the work of any of the authors above but a search through Dickson ((8), p. 164), revealed the work of Euler and Tanturri and I learned of the later work from Pennington himself. Reference to these papers showed that whereas (1) has been proved in a much stronger form the congruence properties (2) appear not to have been noticed before. I was able to prove (2) with the best possible values of k for $n \equiv 0(2)$, $n \equiv 0(4)$, $n \equiv 0(8)$, etc., but a general proof of the best possible result for the case $n \equiv 0(2^m)$ seems to be more difficult.

The object of this paper is to prove a few formulae and results relating to $b(n)$ and to state the unproved conjecture associated with (2) together with some of the evidence supporting it in the hope that someone may be able to find a proof (or disproof).

2. *The binary partition function.* Let $b(0) = 1$ and for $n \geqslant 1$ let $b(n)$ denote the number of ways of expressing n as the sum of powers of 2 (sums which are the same apart from a permutation of the elements are considered to be identical). Thus

$$7 = 1+1+1+1+1+1+1 = 1+1+1+1+1+2 = 1+1+1+2+2$$
$$= 1+2+2+2 = 1+1+1+4 = 1+2+4$$

and so $b(7) = 6$. If for $|x| < 1$ we define

$$F(x) = \sum_{n=0}^{\infty} b(n)\, x^n \tag{1}$$

then, clearly
$$F(x) = \prod_{k=0}^{\infty} (1-x^{2^k})^{-1} \tag{2}$$
and it follows at once from this that $F(x)$ satisfies the functional equation
$$(1-x)F(x) = F(x^2). \tag{3}$$
From (1) and (3) we deduce
$$b(2n+1) = b(2n), \tag{4}$$
$$b(2n) = b(2n-2)+b(n). \tag{5}$$
By repeated application of (4) and (5) we find
$$b(2n) = \sum_{k=0}^{n} b(k). \tag{6}$$
This is a special case of a class of formulae which enable us to express $b(2^m n)$ as a sum involving the numbers $b(n), b(n-1), \ldots, b(0)$.

THEOREM 1. *For any integer $m \geqslant 1$ it is possible to express $b(2^m n)$ in terms of a linear combination of the numbers $b(n), b(n-1), \ldots, b(0)$*
$$b(2^m n) = \sum_{i=0}^{n} C_{m,i}\, b(n-i).$$
The coefficients $C_{m,i}$ are positive integers and
$$C_{1,i} = 1 \quad \textit{for all} \quad i \geqslant 0,$$
$$C_{m+1,i} = \sum_{j=0}^{2i} C_{m,j} \quad \textit{for all} \quad m \geqslant 1.$$

Proof. For $m = 1$ we have already seen that the first part of the theorem holds and that $C_{1,i} = 1$.

Suppose the theorem holds for $m = s$ where $s \geqslant 1$, then
$$b(2^s n) = \sum_{i=0}^{n} C_{s,i}\, b(n-i)$$
and so
$$\begin{aligned} b(2^{s+1}n) = b(2^s.2n) &= \sum_{i=0}^{2n} C_{s,i}\, b(2n-i) \\ &= C_{s,0}\, b(2n) + \sum_{j=1}^{n} (C_{s,2j-1}+C_{s,2j})\, b(2n-2j) \quad \text{from (4)} \\ &= C_{s,0} \sum_{k=0}^{n} b(k) + \sum_{j=1}^{n} \left((C_{s,2j-1}+C_{s,2j}) \sum_{k=0}^{n-j} b(k) \right) \quad \text{from (6)} \\ &= \sum_{k=0}^{n} \sum_{j=0}^{2k} C_{s,j}\, b(n-k). \end{aligned}$$
Hence
$$b(2^{s+1}n) = \sum_{i=0}^{n} C_{s+1,i}\, b(n-i)$$
where
$$C_{s+1,i} = \sum_{j=0}^{2i} C_{s,j}$$
and the theorem follows by induction.

By using the theorem we can work out a table of the values of the coefficients $C_{m,i}$. A section of this table for $1 \leqslant m \leqslant 5$ and $1 \leqslant i \leqslant 7$ is shown below. The table can be used to express $b(2^k n)$ as the sum of $b(n), b(n-1)$, etc., for example

$$b(32n) = b(n) + 201b(n-1) + 1625b(n-2) + \ldots.$$

$m \backslash i$	0	1	2	3	4	5	6
1	1	1	1	1	1	1	1
2	1	3	5	7	9	11	13
3	1	9	25	49	81	121	169
4	1	35	165	455	969	1,771	2,925
5	1	201	1,625	6,321	17,361	38,841	75,881

We now use the first two lines of the table to prove

THEOREM 2.
(i) $b(n) \equiv 0 (\text{mod } 2)$ *for all* $n \geqslant 2$;
(ii) $b(n) \equiv 0 (\text{mod } 4)$ *if and only if* n *or* $n-1 = 4^m . (2k+1), m \geqslant 1$;
(iii) $b(n) \equiv 0 (\text{mod } 8)$ *for no value of* n.

Proof. (i) $b(0) = b(1) = 1$; $b(2) = b(3) = 2$. Suppose $b(m) \equiv 0 (\text{mod } 2)$ for all m in $\langle 2, 2n-1 \rangle$ where $n \geqslant 2$ then

$$b(2n+1) = b(2n) = b(2n-2) + b(n) \equiv 0 \quad (\text{mod } 2)$$

since n and $2n-2$ lie in the interval $\langle 2, 2n-1 \rangle$. Thus the interval is extended to $\langle 2, 2n+1 \rangle$ and the result follows by induction.

(ii) We write $n = 4^m . s$ where $m \geqslant 0$ and $s \not\equiv 0$ (mod 4).

Case 1. $m > 1$. In this case $n = 4^m s = 4P$, say, where $P \equiv 0 (\text{mod } 4)$. The second row of the table gives us the reduction formula

$$b(n) = b(4P) = b(P) + 3b(P-1) + 5b(P-2) + \ldots + (2P-1) b(1) + (2P+1) b(0).$$

Since P is even $b(P-1) = b(P-2)$, $b(P-3) = b(P-4)$, etc., hence

$$b(4P) = b(P) + 8b(P-2) + 16b(P-4) + \ldots + 4Pb(0)$$

and so
$$b(4P) \equiv b(P) \quad (\text{mod } 8).$$

Hence, for $m > 1$

$$b(4^m . s) \equiv b(4^{m-1} . s) \quad (\text{mod } 8). \tag{7}$$

We note that (7) is valid also if $m = 1$ provided s is even. The analysis is exactly the same as above. We now analyse this case further.

Case 2. $m = 1$, $s \equiv 0 (\text{mod } 2)$. Since $s \not\equiv 0$ (mod 4) we can write $s = 4t + 2$. From (7)

$$b(4s) \equiv b(s) \quad (\text{mod } 8).$$

From (5)
$$b(s) = b(4t+2) = b(4t) + b(2t+1) = b(4t) + b(2t).$$

Now
$$b(4t) = b(t) + 3b(t-1) + 5b(t-2) + \ldots$$

and
$$b(2t) = b(t) + b(t-1) + b(t-2) + \ldots.$$

Hence $$b(s) = 2b(t)+4b(t-1)+6b(t-2)+\ldots+2tb(1)+(2t+2)\,b(0).$$

Since $b(r) \equiv 0(2)$ for all $r \geqslant 2$ it follows that

$$b(s) = b(4t+2) \equiv (4t+2) \equiv 2 \pmod 4. \tag{8}$$

Combining (7) and (8) we deduce, for all $m \geqslant 0$

$$b(4^m(4t+2)) \equiv 2 \pmod 4. \tag{9}$$

Case 3. $m = 1$, $s \equiv 1, 3 \pmod 4$. We now have $s \equiv 1 \pmod 2$ and so

$$\begin{aligned} b(4s) &= b(s)+3b(s-1)+5b(s-2)+\ldots+(2s-1)\,b(1)+(2s+1)\,b(0) \\ &= 4b(s-1)+12b(s-3)+\ldots+4sb(0) \end{aligned}$$

whence $$b(4s) \equiv 4s \pmod 8 \equiv 4 \pmod 8$$
since s is odd.

Thus we have proved that

$$b(n) \equiv 4 \pmod 8 \quad \text{if} \quad n = 4^m.(2k+1) \quad \text{and} \quad m \geqslant 1 \tag{10}$$

and we have also proved that

$$b(n) \equiv 2 \pmod 4 \quad \text{if} \quad n = 4^m.(4t+2) \quad \text{and} \quad m \geqslant 0. \tag{11}$$

The only remaining case is $n = (2k+1)$ but this case reduces to (10) and (11) since $b(2k+1) = b(2k)$.

Combining (10) and (11) we see that

$$b(n) \equiv 4 \pmod 8 \equiv 0 \pmod 4 \quad \text{if and only if} \quad n = 4^m.(2k+1) \quad \text{if } n \text{ is even}$$

$$\text{or} \quad n-1 = 4^m.(2k+1) \quad \text{if } n \text{ is odd}$$

and $b(n) \equiv 2 \pmod 4$ for all other $n \geqslant 2$. Thus in no case is $b(n) \equiv 0(8)$ and (ii) and (iii) of the theorem are proved.

3. *The conjecture.* We established in (7) that $b(4s) \equiv b(s) \pmod 8$ if s is even. By writing $s = 2t$ we see that we have proved that, for all t

$$b(8t)-b(2t) \equiv 0 \pmod 8. \tag{12}$$

Similarly, it can be proved that, for all t

$$b(16t)-b(4t) \equiv 0 \pmod{32} \tag{13}$$

and other results of the same kind. Each result can be proved by using the coefficients of Table 1 to express $b(2^k t)$ as a sum involving $b(t), b(t-1), \ldots, b(0)$ and also to express $b(2^{k-2}t)$ as a sum of the same type. The numerical evidence indicates that such congruence properties hold for arbitrarily large values of k and this leads to

Conjecture. If $k \geqslant 1$ and $t \equiv 1 \pmod 2$

$$b(2^{2k+2}t)-b(2^{2k}t) \equiv 0 \pmod{2^{3k+2}},$$

$$b(2^{2k+1}t)-b(2^{2k-1}t) \equiv 0 \pmod{2^{3k}}.$$

The evidence further indicates that these congruences hold *exactly*, i.e. that no higher power of 2 divides $b(4n) - b(n)$. Thus, for example

$$b(2^{10}) - b(2^8) = 2{,}320{,}518{,}948 - 692{,}004 = 141{,}591 \times 2^{14}$$

and $$b(7.2^7) - b(7.2^5) = 962{,}056{,}258 - 355{,}906 = 1{,}878{,}321 \times 2^9$$

and $$b(3.2^8) - b(3.2^6) = 357{,}547{,}444 - 169{,}396 = 174{,}501 \times 2^{11}$$

and $$b(53.2^4) - b(53.2^2) = 673{,}353{,}212 - 272{,}156 = 21{,}033{,}783 \times 2^5.$$

In each case the power of 2 is precisely the one predicted by the conjecture.

A table of values of $b(n)$ is given at the end of the paper.

4. *Partitions of powers of other integers.* I have also used the computer to study the number of partitions, $t(n)$, of n as a sum of powers of an integer $m > 2$. There is, in general, no simple equivalent of Theorem 2. Theorem 1 and the conjecture carry through to a considerable extent though the precise form of the conjecture depends upon whether m is prime or composite. The strongest congruences usually involve the difference $t(m^{r+1}.k) - t(m^r.k)$, rather than $t(m^{r+2}.k) - t(m^r.k)$ which is what one might expect from the case $m = 2$. Also the (suspected) property of *exact* divisibility by a power of 2 does not carry over to exact divisibility by a power of m. For example, if $m = 3$ and $t(n)$ denotes partitions of n as a sum of powers of 3 then

$$t(9) - t(3) = 3, \quad t(27) - t(9) = 2\cdot 3^2, \quad t(81) - t(27) = 2^3.3^3$$

and $$t(243) - t(81) = 23\cdot 3^5, \tag{14}$$

whereas $$t(4\cdot 243) - t(4\cdot 81) = 173.3^8 \tag{15}$$

and yet $$t(729) - t(243) = 5^3.11.3^5. \tag{16}$$

From (14), (15), (16) it appears that any conjecture corresponding to the one above is unlikely to predict the exact power of m which divides $t(m^{r+1}.k) - t(m^r.k)$ for $m \geqslant 3$.

REFERENCES

(1) Euler, L. *Novi Comm. Petrop.* III (1750).

(2) Tanturri, A. *Atti Accad. Sci. Torino Cl. Sci. Fis. Mat. Natur.* **52** (1916), 902–908.

(3) Tanturri, A. *Atti Accad. Sci. Torino Cl. Sci. Fis. Mat. Natur.* **54** (1918), 69–82.

(4) Tanturri, A. *Atti. Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez I.* **27** (1918), 399–403.

(5) Mahler, K. *J. London Math. Soc.* **15** (1940), 115–123.

(6) De Bruijn, N. G. *Nederl. Akad. Wetensch. Proc. Ser. A* **51** (1948), 659–669.

(7) Pennington, W. B. *Ann. of Math.* **57** (1953), 531–546.

(8) Dickson, L. E. *History of the theory of numbers*, vol. 2 (1952) (Chelsea Publishing Co., New York, 1952).

Table 1. *Values of the binary partition function*

n	$b(n)$	n	$b(n)$
0	1		
2	2	102	10,614
4	4	104	11,514
6	6	106	12,414
8	10	108	13,428
10	14	110	14,442
12	20	112	15,596
14	26	114	16,750
16	36	116	18,044
18	46	118	19,338
20	60	120	20,798
22	74	122	22,258
24	94	124	23,884
26	114	126	25,510
28	140	128	27,338
30	166	130	29,166
32	202	132	31,196
34	238	134	33,226
36	284	136	35,494
38	330	138	37,762
40	390	140	40,268
42	450	142	42,774
44	524	144	45,564
46	598	146	48,354
48	692	148	51,428
50	786	150	54,502
52	900	152	57,906
54	1014	154	61,310
56	1154	156	65,044
58	1294	158	68,778
60	1460	160	72,902
62	1626	162	77,026
64	1828	164	81,540
66	2030	166	86,054
68	2268	168	91,018
70	2506	170	95,982
72	2790	172	101,396
74	3074	174	106,810
76	3404	176	112,748
78	3734	178	118,686
80	4124	180	125,148
82	4514	182	131,610
84	4964	184	138,670
86	5414	186	145,730
88	5938	188	153,388
90	6462	190	161,046
92	7060	192	169,396
94	7658	194	177,746
96	8350	196	186,788
98	9042	198	195,830
100	9828	200	205,658