Math. Proc. Camb. Phil. Soc. (1975), **78**, 437
MPCPS 78–40
Printed in Great Britain

Congruence properties of the binary partition function

BY M. D. HIRSCHHORN AND J. H. LOXTON
School of Mathematics, University of New South Wales, Kensington, N.S.W., Australia

(*Received* 19 *December* 1974)

1. *Introduction.* We denote by $b(n)$ the number of binary partitions of n, that is the number of partitions of n as the sum of powers of 2. As usual, two partitions are not considered to be distinct if they differ only in the order of their summands. It is convenient to define $b(0) = 1$.

The function $b(n)$ was investigated by Euler, but Churchhouse (1) seems to have been the first to observe that it possesses simple congruence properties modulo 2, 4 and 8, namely

$$b(n) \equiv 0 \pmod 2 \quad \text{for} \quad n \geqslant 2,$$

$$b(n) \equiv 0 \pmod 4 \text{ if and only if } n \text{ or } n-1 = 4^r(2k+1) \text{ with } r \geqslant 1, \text{ and}$$

$$b(n) \not\equiv 0 \pmod 8.$$

He also conjectured that if $r \geqslant 1$ and $n \equiv 1 \pmod 2$, then

$$\left.\begin{aligned} b(2^{2r+2}n) - b(2^{2r}n) &\equiv 2^{3r+2} \pmod{2^{3r+3}} \\ \text{and} \qquad b(2^{2r+1}n) - b(2^{2r-1}n) &\equiv 2^{3r} \pmod{2^{3r+1}}. \end{aligned}\right\} \tag{1}$$

These congruences were proved by Gupta (2) and Rödseth (3).

The aim of this note is to continue these investigations and, in fact, to give a complete list of all the congruences of a certain type satisfied by $b(n)$. For this purpose, we introduce two functions $\lambda(n)$ and $\mu(n)$ defined for a positive integer n as follows:

$\lambda(n) = 1$ or -1 according as the binary expansion of n ends in an even or odd number of zeros, and

$\mu(n) = 1$ or -1 according as the binary expansion of n contains an even or odd number of ones.

We also define $\mu(0) = 1$. The 'admissible congruence for $b(n)$' are congruences of the shape

$$b(2^r n + t) \equiv X(n) \pmod{2^k} \quad (n \geqslant 1),$$

where $0 \leqslant t < 2^r$ and $X(n)$ is a function which depends on n only through $\lambda(n)$ and $\mu(n)$. If, in the above congruence, we restrict n to the progression $n = 2^s m + u$, where $0 \leqslant u < 2^s$, we obtain another admissible congruence

$$b(2^{r+s}m + 2^r u + t) \equiv X(m) \pmod{2^k} \quad (m \geqslant 1),$$

https://doi.org/10.1017/S0305004100051896 Published online by Cambridge University Press

possibly with a different function X, since $\lambda(2^s m+u)$ and $\mu(2^s m+u)$ are readily expressed in terms of $\lambda(m)$ and $\mu(m)$ thus

$$\lambda(2^s m+u)=\begin{cases}(-1)^s\lambda(m) & \text{if } u=0\\ \lambda(u) & \text{otherwise,}\end{cases}$$

and

$$\mu(2^s m+u)=\mu(u)\mu(m).$$

An admissible congruence which does not arise in this way from another one, we call 'primitive'. With this terminology, we can state the main result.

THEOREM. *The binary partition function, $b(n)$, satisfies*

$$b(2n)\equiv 1+\lambda(n) \pmod 4 \quad (n\geqslant 1),$$

$$b(4n+2)\equiv 2\mu(n) \pmod 8,$$

$$b(8n)\equiv \mu(n)\{1-3\lambda(n)\} \pmod 8 \quad (n\geqslant 1), \tag{2}$$

$$b(8n+2)\equiv 2\mu(n) \pmod{16}, \tag{3}$$

$$b(8n+4)\equiv 4 \pmod 8,$$

$$b(8n+6)\equiv 6\mu(n) \pmod{16}, \tag{4}$$

$$b(2^{2r}n+2^{2r-2})\equiv 4\mu(n) \pmod{32} \quad (r\geqslant 2),$$

$$b(2^{2r}n+3.2^{2r-2})\equiv 20\mu(n) \pmod{32} \quad (r\geqslant 2),$$

$$b(2^{2r+1}n+2^{2r-1})\equiv 10\mu(n) \pmod{16} \quad (r\geqslant 2),$$

and

$$b(2^{2r+1}n+3.2^{2r-1})\equiv 14\mu(n) \pmod{16} \quad (r\geqslant 2).$$

These congruences, together with those which follow from the equation $b(2n+1)=b(2n)$, are the only primitive admissible congruences for $b(n)$.

2. *Preliminary results.* Following Euler, we introduce the function

$$F(x)=\sum_{n=0}^{\infty} b(n)x^n=\prod_{n=0}^{\infty}(1-x^{2^n})^{-1}. \tag{5}$$

Clearly, $F(x)$ satisfies the functional equation

$$(1-x)F(x)=F(x^2),$$

so we find the recurrence relations

$$\left.\begin{aligned} b(2n+1)&=b(2n)\\ \text{and}\quad b(2n)&=b(2n-2)+b(n).\end{aligned}\right\} \tag{6}$$

From the first of these, we need only consider $b(n)$ for even values of n. From the second, it follows easily that $b(n)\equiv 0 \pmod 2$ for $n\geqslant 2$. A table of values of $b(n)$ for even values of n up to 100 is given at the end of the paper.

The succeeding arguments will be based on four lemmas.

LEMMA 1. *Let r, t be integers with $r\geqslant 4$, $0<t<2^{r-1}$ and $t\equiv 0 \pmod 2$. Then*

$$b(2^r n)\equiv b(4n) \quad \text{or} \quad b(8n) \pmod{32}, \quad \text{according as } r \text{ is even or odd},$$

$$b(2^r n+2^{r-1})\equiv\begin{cases} b(4n+2)+8 \pmod{16} & (r \text{ even})\\ b(8n+4) \pmod{32} & (r \text{ odd})\end{cases}$$

and

$$b(2^r n\pm t)\equiv \tfrac{1}{2}(\pm 1)^{r-1}b(t)\,b(8n\pm 2) \pmod{32}.$$

https://doi.org/10.1017/S0305004100051896 Published online by Cambridge University Press

Proof. The first two congruences follow easily from (1). We prove the third by induction on r and t. Firstly, it is readily checked for $r = 4$ using (6) and the first congruence of the lemma. Suppose it to hold for some $r \geqslant 4$. Then

$$\begin{aligned} b(2^{r+1}n \pm 2) &= b(2^{r+1}n) \pm b(2^r n), \quad \text{by (6)}, \\ &\equiv b(2^{r-1}n) \pm b(2^r n) \pmod{32}, \quad \text{by (1)}, \\ &= \pm b(2^r n \pm 2), \quad \text{by (6)}, \\ &\equiv (\pm 1)^r b(8n \pm 2) \pmod{32}, \end{aligned}$$

by the induction hypothesis. Suppose, further, that for some t with $0 < t < 2^r - 2$, we have

$$b(2^{r+1}n \pm t) \equiv \tfrac{1}{2}(\pm 1)^r b(t)\, b(8n \pm 2) \pmod{32},$$

and set $u = 0$ or 1 according as $t \equiv 0$ or $2 \pmod 4$. Then

$$\begin{aligned} b(2^{r+1}n \pm (t+2)) &= b(2^{r+1}n \pm t) \pm b(2^r n \pm (\tfrac{1}{2}t + u)) \\ &\equiv \tfrac{1}{2}(\pm 1)^r \{b(t) + b(\tfrac{1}{2}t + u)\}\, b(8n \pm 2) \pmod{32} \\ &= \tfrac{1}{2}(\pm 1)^r b(t+2)\, b(8n \pm 2). \end{aligned}$$

Hence the desired result follows by induction.

LEMMA 2. *Let r, t be integers with $r \geqslant 5$, $0 < t < 2^{r-2}$ or $2^{r-2} < t < 2^{r-1}$, and $t \equiv 0 \pmod 2$. Then*

$$b(2^r n \pm 2^{r-2}) \equiv \begin{cases} b(16n \pm 4) + 32 \pmod{64} & (r \text{ even}) \\ b(32n \pm 8) \pmod{64} & (r \text{ odd}) \end{cases}$$

and

$$b(2^r n \pm t) \equiv \tfrac{1}{2}(\pm 1)^r b(t)\, b(16n \pm 2) \pmod{64}.$$

Proof. The first congruence follows from (1). For the second, we proceed by induction on r and t as in the proof of Lemma 1. The result is easily checked for $r = 5$. Suppose it holds for some $r \geqslant 5$. As before, we have

$$b(2^{r+1}n \pm t) \equiv \tfrac{1}{2}(\pm 1)^{r+1} b(t)\, b(16n \pm 2) \pmod{64}, \tag{7}$$

providing $0 < t < 2^{r-1}$. Now

$$\begin{aligned} b(2^{r+1}n \pm (2^{r-1} + 2)) &= b(2^{r+1}n \pm 2^{r-1}) \pm b(2^r n \pm 2^{r-2}) \\ &= b(2^{r+1}n \pm (2^{r-1} - 2)) \pm 2b(2^r n \pm 2^{r-2}) \\ &\equiv \tfrac{1}{2}(\pm 1)^{r+1} \{b(2^{r-1} - 2) + 2b(2^{r-2})\}\, b(16n \pm 2) \pmod{64} \\ &= \tfrac{1}{2}(\pm 1)^{r+1} b(2^{r-1} + 2)\, b(16n \pm 2), \end{aligned}$$

where, in the penultimate step, we have used Lemma 1 and (7) with $t = 2^{r-1} - 2$. From this, we obtain (7) for the remaining values of t with $2^{r-1} < t < 2^r$ by induction, and this completes the proof.

LEMMA 3.

$$\sum_{n=0}^{\infty} b(8n)\, x^n = (1 + 6x + x^2)\, F(x)/(1-x)^3,$$

$$\sum_{n=0}^{\infty} b(8n+2)\, x^n = 2(1 + 3x)\, F(x)/(1-x)^3$$

https://doi.org/10.1017/S0305004100051896 Published online by Cambridge University Press

and
$$\sum_{n=0}^{\infty} b(8n+6)\,x^n = 2(3+x)\,F(x)/(1-x)^3.$$

Proof. From the definition (5) of $F(x)$, we see that

$$\sum_{n=0}^{\infty} b(n)\,x^n = (1+x)\,(1+x^2)^2\,(1+x^4)^3\,F(x^8)/(1-x^8)^3.$$

After multiplying out the first three factors and picking out the terms in x^{8n}, we obtain

$$\sum_{n=0}^{\infty} b(8n)\,x^{8n} = (1+6x^8+x^{16})\,F(x^8)/(1-x^8)^3,$$

which is the first of the stated generating functions. The others follow in the same way.

LEMMA 4.
$$\sum_{n=0}^{\infty} \mu(n)\,x^n = \prod_{n=0}^{\infty} (1-x^{2^n})$$

and
$$\sum_{n=1}^{\infty} \lambda(n)\,\mu(n)\,x^n = -x \prod_{n=0}^{\infty} (1-x^{2^n}).$$

Proof. If the product $\Pi(1-x^{2^n})$ is multiplied out, the term in x^n occurs with coefficient 1 or -1 according as the binary expansion of n contains an even or odd number of ones. This proves the first equation of the lemma and the second follows at once since $\lambda(n)\,\mu(n) = -\mu(n-1)$.

3. *Proof of the congruences.* We can now prove the congruences stated in the theorem. First, note that it is enough to prove the congruences (2), (3) and (4) for $b(8n)$, $b(8n+2)$ and $b(8n+6)$ respectively. The congruences for $b(16n+4)$, $b(16n+12)$, $b(32n+8)$ and $b(32n+24)$ then follow from Lemma 1 and those for $b(2^r n+2^{r-2})$ and $b(2^r n+3\cdot 2^{r-2})$ with $r \geqslant 6$ from Lemma 2. The remaining congruences are easy consequences of all those so far established and the recurrence relations (6).

By an easy induction on n, we have

$$(1-x)^5\,(1-x^2)^2 \ldots (1-x^{2^n})^2 \equiv 1+3x+2x^{2^{n+1}}-2x^{2^{n+1}+1}-3x^{2^{n+2}}-x^{2^{n+2}+1} \pmod 8.$$

On letting $n \to \infty$ in this, we get the formal power series congruence

$$(1-x)^5\,(1-x^2)^2\,(1-x^4)^2\,(1-x^8)^2 \ldots \equiv 1+3x \pmod 8. \tag{8}$$

From Lemmas 3 and 4,

$$\begin{aligned}\sum_{n=1}^{\infty} [b(8n)-\mu(n)\{1-3\lambda(n)\}]\,x^n &= \left\{(1+6x+x^2)-(1+3x)\,(1-x)^5 \prod_{n=1}^{\infty}(1-x^{2^n})^2\right\} F(x)/(1-x)^3 \\ &\equiv 0 \pmod 8,\end{aligned}$$

from (8), since $1+6x+x^2 \equiv (1+3x)^2 \pmod 8$. This proves (2). Similarly,

$$\begin{aligned}\sum_{n=0}^{\infty} [b(8n+2)-2\mu(n)]\,x^n &= 2\left\{(1+3x)-(1-x)^5 \prod_{n=1}^{\infty}(1-x^{2^n})^2\right\} F(x)/(1-x)^3 \\ &\equiv 0 \pmod{16},\end{aligned}$$

https://doi.org/10.1017/S0305004100051896 Published online by Cambridge University Press

giving (3), and

$$\sum_{n=0}^{\infty}[b(8n+6)-6\mu(n)]x^n = 2\left\{(3+x)-3(1-x)^5\prod_{n=1}^{\infty}(1-x^{2^n})^2\right\}F(x)/(1-x)^3$$
$$\equiv 0 \pmod{16},$$

giving (4). This proves the positive half of the theorem.

4. *Completion of the proof.* It remains to prove that the list of congruences in the theorem is complete, and for that purpose we must eliminate five types of hypothetical congruences. In the following, we denote by $X(n)$ a function which depends on n only through $\lambda(n)$ and $\mu(n)$, but which may possibly be a different function at each occurrence.

First case. Congruences for $b(2^rn)$. Suppose $b(2^rn) \equiv X(n) \pmod{16}$ with $r \geqslant 4$. From Lemma 1, this gives $b(8n) \equiv X(n) \pmod{16}$. Now $\lambda(3) = \lambda(5) = 1$ and $\mu(3) = \mu(5) = 1$, so we require $b(24) \equiv b(40) \pmod{16}$. The last congruence is, however, false. (See the table below.)

Second case. Congruences for $b(2^rn+2^{r-1})$. Suppose $b(2^rn+2^{r-1}) \equiv X(n) \pmod{16}$ with $r \geqslant 4$. From Lemma 1, this gives $b(4n+2)$ or $b(8n+4) \equiv X(n) \pmod{16}$. Now $\lambda(1) = \lambda(4) = 1$ and $\mu(1) = \mu(4) = -1$, so we require $b(6) \equiv b(18)$ or $b(12) \equiv b(36) \pmod{16}$. However, both these congruences are false.

Third case. Congruences for $b(2^rn+t)$ with $\lambda(t) = -1$. Suppose $b(2^rn+t) \equiv X(n) \pmod{32}$ with $r \geqslant 4$, $0 < t < 2^{r-1}$ and $\lambda(t) = -1$. From the first congruence of the theorem, $b(t) \equiv 2 \pmod 4$, so Lemma 1 gives $b(8n+2) \equiv X(n) \pmod{32}$ and, in particular, $b(26) \equiv b(42) \pmod{32}$, on taking $n = 3$ and 5, as in the first case. The last congruence, however, is false. Again, if $b(2^rn+t) \equiv X(n) \pmod{32}$ with $r \geqslant 4$, $2^{r-1} < t < 2^r$ and $\lambda(t) = -1$, then $b(2^rn-(2^r-t)) \equiv X(n-1) \pmod{32}$ and Lemma 1 gives

$$b(8n-2) \equiv X(n-1),$$

that is $b(8n+6) \equiv X(n) \pmod{32}$. Taking $n = 1$ and 4 in this gives $b(14) \equiv b(38) \pmod{32}$, a contradiction.

Fourth case. Congruences for $b(2^rn+2^{r-2})$ and $b(2^rn+3.2^{r-2})$. Suppose

$$b(2^rn+2^{r-2}) \equiv X(n) \pmod{64}$$

with $r \geqslant 5$. From Lemma 2, this gives $b(16n+4)$ or $b(32n+8) \equiv X(n) \pmod{64}$. The second of the two possibilities is impossible from the previous case and taking $n = 1$ and 4 in the first gives $b(20) \equiv b(68) \pmod{64}$, a contradiction. Similarly, if

$$b(2^rn+3.2^{r-2}) \equiv X(n) \pmod{64}$$

with $r \geqslant 5$, we are led to $b(16n+12)$ or $b(32n+24) \equiv X(n) \pmod{64}$. Again, the second possibility is ruled out by the previous case and taking $n = 3$ and 5 in the first gives $b(60) \equiv b(92) \pmod{64}$, a contradiction.

Fifth (and last) case. Congruences for $b(2^rn+t)$ with $\lambda(t) = 1$. Suppose

$$b(2^rn+t) \equiv X(n) \pmod{64}$$

https://doi.org/10.1017/S0305004100051896 Published online by Cambridge University Press

Table 1. *Values of* $b(n)$

n	$b(n)$	n	$b(n)$	n	$b(n)$
0	1	34	238	68	2268
2	2	36	284	70	2506
4	4	38	330	72	2790
6	6	40	390	74	3074
8	10	42	450	76	3404
10	14	44	524	78	3734
12	20	46	598	80	4124
14	26	48	692	82	4514
16	36	50	786	84	4964
18	46	52	900	86	5414
20	60	54	1014	88	5938
22	74	56	1154	90	6462
24	94	58	1294	92	7060
26	114	60	1460	94	7658
28	140	62	1626	96	8350
30	166	64	1828	98	9042
32	202	66	2030	100	9828

with $r \geqslant 5$, $t \equiv 0 \pmod 2$, $0 < t < 2^r$ but $t \neq 2^{r-2}$, 2^{r-1} or 3.2^{r-2}, and $\lambda(t) = 1$. From the theorem, $b(t) \not\equiv 0 \pmod 8$, so using Lemma 2 and reasoning as in the third case, we get $b(16n+2)$ or $b(16n+14) \equiv X(n) \pmod{32}$. Both these congruences are ruled out by the third case.

This completes the proof of the theorem.

REFERENCES

(1) CHURCHHOUSE, R. F. Congruences for the binary partition function. *Proc. Cambridge Philos. Soc.* **66** (1969), 371–376.

(2) GUPTA, H. Proof of the Churchhouse conjecture concerning binary partitions. *Proc. Cambridge Philos. Soc.* **70** (1971), 53–56.

(3) RÖDSETH, Ö. Some arithmetical properties of m-ary partitions. *Proc. Cambridge Philos. Soc.* **68** (1970), 447–453.

https://doi.org/10.1017/S0305004100051896 Published online by Cambridge University Press