A FINITE ANALOGUE OF THE GOLDBACH PROBLEM

J.D. Dixon

(received September 22, 1959)

E. Cohen [1], [2] has considered an analogue of the famous Goldbach problem in certain finite rings. In the following another analogue is considered in the ring J_n of residue classes over the integers modulo n.

As 'primes' in J_n we take all residue classes coprime to n. That is, all elements $p \in J_n$ which are not factors of zero in J_n. We denote this set by R_n.

We define $A(m,n,k)$ to be the number of sets $\{p_1, p_2, \ldots, p_k\}$ with $p_i \in R_n$ which for given m satisfy

$$m \equiv \sum_{i=1}^{k} p_i \pmod n$$

where the order of the p_i is taken into account.

The object of this paper is to derive an explicit expression for $A(m,n,k)$. We consider the case $k = 2$ first (this is the analogue to the original Goldbach problem) and then the case where $k \geq 2$. Also in the sections 1 and 2 we consider only the restricted case when n is 'squarefree' ($\mu(n) \neq 0$) and extend our results to the case of n with multiple factors in section 3.

1. When $k = 1$ it is immediate that

$$(1) \qquad A(m,n,1) = \begin{cases} 0 & \text{if } (m,n) > 1 \\ 1 & \text{if } (m,n) = 1. \end{cases}$$

Part of this work was done while the author was receiving a University Research Grant at the University of Melbourne, Australia.

Can. Math. Bull. vol. 3, no. 2, May 1960.

https://doi.org/10.4153/CMB-1960-013-5 Published online by Cambridge University Press

Now consider the case k = 2. We can then show

(2) $$A(m,n,2)\,A(m,n',2) = A(m,nn',2)$$

provided $(n,n') = 1$. That is, $A(m,n,2)$ is multiplicative in n.

The proof is as follows.

Let $m \equiv p_1 + p_2 \pmod{n}$ with $p_i \in R_n$

and $m \equiv p_1' + p_2' \pmod{n'}$ with $p_i' \in R_{n'}$.

Since $(n,n') = 1$ there exist integers λ, ν which are coprime to n' and n respectively and such that $\lambda n + \nu n' = 1$.

We then define

(3) $$p_i'' \equiv \nu n' p_i + \lambda n p_i' \pmod{nn'}.$$

Clearly
$$\begin{aligned} p_1'' + p_2'' &\equiv \nu n'(p_1 + p_2) + \lambda n(p_1' + p_2') \\ &\equiv \nu n'(m + an) + \lambda n(m + bn') \\ &\equiv m \pmod{nn'} \end{aligned}$$

where a, b are integers and remembering that $\nu n' + \lambda n = 1$.

Furthermore (3) defines p_i'' uniquely (mod nn') in terms of p_i, p_i' and conversely p_i, p_i' are uniquely determined (mod n) and (mod n') respectively, by $p_i \equiv p_i'' \pmod{n}$ and $p_i' \equiv p_i'' \pmod{n'}$. There is, therefore, a one-one correspondence between the sets $\{p_1'', p_2''\}$ and the pairs of sets $\{p_1, p_2\}$, $\{p_1', p_2'\}$. Since it can be seen that $(p_i'', nn') = 1$ equation (2) follows.

Under the assumption that n is 'squarefree' we may write $n = q_1 q_2 \ldots q_s$ where the q_i are distinct prime numbers. Then applying (2) we may write

(4) $$A(m,n,2) = \prod_{q|n} A(m,q,2) .$$

By considering the number of solutions to $p_2 \equiv m - p_1 \pmod{q}$ in each of the cases where p_1 takes a particular value from the set $R_q = \{1, 2, \ldots, q-1\}$ it is seen that

$$A(m,q,2) = \sum_{p_1 \in R_q} A(m-p_1,q,1) = \sum_{p_1=1}^{q-1} A(m-p_1,q,1)$$

and that therefore

(5) $$A(m,q,2) = \sum_{r=0}^{q-1} A(r,q,1) - A(m,q,1).$$

For any prime number q (5) and (1) give

$$A(m,q,2) = (q-1) - A(m,q,1) ,$$

(6) $$A(m,q,2) = \begin{cases} (q-2) & \text{if } q \nmid m \\ (q-1) & \text{if } q \mid m . \end{cases}$$

So substituting (6) in (4) we finally get (remembering that n is 'squarefree')

(7) $$A(m,n,2) = \prod_{q|(m,n)} (q-1) \prod_{q|n/(m,n)} (q-2)$$

where the first product is over primes dividing both n and m and the second over primes dividing n but not m.

2. In the general case of $k \geqslant 2$ but still restricting $\mu(n) \neq 0$ we find in a similar way the following formulae corresponding to (4) and (5).

(4)* $A(m,n,k) = \prod_{q|n} A(m,q,k)$ when $\mu(n) \neq 0$,

(5)* $A(m,q,k) = \sum_{r=0}^{q-1} A(r,q,k-1) - A(m,q,k-1)$ when q is prime.

We now evaluate $A(m,q,k)$ from the recurrence relation (5)*. Put $S(q,k) = \sum_{r=0}^{q-1} A(r,q,k-1)$. Summing (5)* over m from 0 to $q-1$,

$$S(q,k) = q\,S(q,k-1) - S(q,k-1)$$

$$= (q-1)\,S(q,k-1).$$

But from (1) $S(q,1) = q-1$ so by induction on k, $S(q,k) = (q-1)^k$ which substituted into (5)* gives

(8) $$A(m,q,s) = (q-1)^{s-1} - A(m,q,s-1).$$

Summing (8) over s

https://doi.org/10.4153/CMB-1960-013-5 Published online by Cambridge University Press

$$\sum_{s=2}^{k} (-1)^s A(m,q,s) = \sum_{s=2}^{k} (-1)^s (q-1)^{s-1} - \sum_{s=2}^{k} (-1)^s A(m,q,s-1).$$

So

$$\sum_{s=2}^{k} (-1)^s A(m,q,s) - \sum_{s=1}^{k-1} (-1)^s A(m,q,s) = - \sum_{s=1}^{k-1} (-1)^s (q-1)^s$$

and hence

$$(-1)^k A(m,q,k) + A(m,q,1) = 1 - \frac{1}{q}\{(-1)^k (q-1)^k - 1\}.$$

Therefore

(9) $$A(m,q,k) = \frac{1}{q}\{(q-1)^k - (-1)^k\} + (-1)^k (1 - A(m,q,1)) .$$

So applying (1)

(10) $$A(m,q,k) = \begin{cases} \frac{1}{q}\{(q-1)^k - (-1)^k\} & \text{if } q \nmid m \\ \frac{q-1}{q}\{(q-1)^{k-1} - (-1)^{k-1}\} & \text{if } q \mid m \end{cases}$$

which is the generalisation of (6).

So for n 'squarefree' (4)* and (10) give

(11) $A(m,n,k)$

$$= \prod_{q|(m,n)} \frac{q-1}{q}\{(q-1)^{k-1} - (-1)^{k-1}\} \prod_{q|n/(m,n)} \frac{1}{q}\{(q-1)^k - (-1)^k\}.$$

3. We now remove the restriction that n is 'squarefree'. Write $n = hn'$ where $n' = \prod_{q|n} q$ satisfies $\mu(n') \neq 0$.

Since the 'primes' of J_n are simply the residue classes coprime to n' it is seen that $R_n = \{p'+rn' \mid p' \in R_{n'},\ r \in \{0,1,.,h-1\}\}$.

If $\{p_1, p_2, \ldots, p_k\}$ is a set of $p_i \in R_n$ which satisfies

(12) $$m \equiv \sum_{i=1}^{k} p_i \pmod{n}$$

we must have

(13) $$m \equiv \sum_{i=1}^{k} p_i' \pmod{n'}$$

where $p_i' \equiv p_i \pmod{n'}$ and $p_i' \in R_{n'}$.

https://doi.org/10.4153/CMB-1960-013-5 Published online by Cambridge University Press

So

$$m \equiv \sum_{i=1}^{k} p_i' + r(m)n' \qquad (\text{mod } n)$$

for some $r(m)$.

And the number of solutions (12) corresponding to each solution (13) is the number of sets $\{r_1, r_2, \ldots, r_k\}$ with $r_i \in \{0, 1, \ldots, h-1\}$ which satisfy

$$r(m)n' \equiv \sum_{i=1}^{k} r_i n' \qquad (\text{mod } n)$$

and hence

$$r(m) \equiv \sum_{i=1}^{k} r_i \qquad (\text{mod } h)$$

since $n = n'h$.

But to solve this congruence we may arbitrarily choose $r_1, r_2, \ldots, r_{k-1}$ and then r_k is determined. Therefore for each solution (13) there are h^{k-1} solutions (12).

Therefore we have shown

(14) $$A(m,n,k) = h^{k-1} A(m,n',k)$$

where n' is the largest 'squarefree' divisor of n and $h = n/n'$.

4. Finally we ask in what cases $A(m,n,k) = 0$. Since the cases with $k = 1$ are already given by (1) we take $k \geqslant 2$. Then by (11) $A(m,n,k) = 0$ if and only if for some prime $q \mid n$:

(i) $\quad (q-1)^{k-1} = (-1)^{k-1} \quad$ when $q \mid m$

or

or (ii) $\quad (q-1)^{k} = (-1)^{k} \quad$ when $q \nmid m$.

Since the left hand sides of these equations are both of magnitude greater than unity for $q \geqslant 3$ we must have $q = 2$ in order that $A(m,n,k) = 0$. Further we require k to be even when $2 \nmid m$ and to be odd when $2 \mid m$. (Cases (ii) and (i) respectively) We can therefore say $A(m,n,k)$ is strictly positive for $k \geqslant 2$ except when n is even and m and k have opposite parity.

https://doi.org/10.4153/CMB-1960-013-5 Published online by Cambridge University Press

REFERENCES

1. E. Cohen, A finite analogue to the Goldbach problem, Proc. Amer. Math. Soc. 5 (1954), 478 - 483.

2. ...., The finite Goldbach problem in algebraic number fields, Proc. Amer. Math. Soc. 7 (1956), 500 - 506.

McGill University