Congruence properties of self-contained balanced sets

By Hansraj Gupta.

(*Received* 10*th June*, 1938. *Read* 4*th November*, 1938.)

1. Let the set $b_1, b_2, b_3, \ldots, b_k$; of k non-negative integers be denoted by B_k. Let ξB_k denote the set $\xi b_1, \xi b_2, \xi b_3, \ldots, \xi b_k$; ξ being any integer > 1. Without loss of generality, we can suppose that $b \leqq b_{i+1}$.

In what follows, $G_r(B_k)$ denotes the sum of the products taken r at a time of the members of set B_k; $0 \leqq r \leqq k$. We take $G_0(B_k) = 1$. $S_r(B_k)$ stands for the sum of the r-th powers of the members of set B_k. All small letters denote integers $\geqq 0$, unless stated otherwise; p's denote primes $\geqq 2$; $m > 2$; and ϕ is Euler's function.

If $m \equiv 0 \pmod{p^u}$, but $\not\equiv 0 \pmod{p^{u+1}}$, $u > 0$, then we say that m is u-potent in p, and write $\text{Pot}_p\, m = u$. In the same way, when $\phi(p^a) \mid g$, but $\phi(p^{a+1})$ does not divide g, $a > 0$, then we say that g is a-piquant in p, and write $\text{Piq}_p\, g = a$. Evidently if $\text{Piq}_p\, g = a$, then $\text{Pot}_p\, g = a - 1$, but not conversely. Again if $\text{Piq}_p\, g = a > 0$, then we write M_g for the product $\Pi\, (p^{a+[2/p]})$, and N_g for the product $\prod_{a>0} (p^{1+[2/p]})$. Thus $N_6 = 7.3.2^2$, and $M_6 = 7.3^2.2^3$.

A set B_k is said to be self-contained modulo m, when for every number ξ less than and prime to m, the members of set ξB_k are congruent modulo m to the members of set B_k, each to each, though not necessarily in the same order.

If the members of set B_k satisfy the relation:

$$b_i + b_{k-i+1} = m, \qquad i = 1, 2, 3, \ldots, k;$$

then B_k is called a balanced m-set.

2. We make use of the following

Lemma. *If* $\text{Piq}_p\, g = a$, *then numbers* ξ *prime to* p, *exist such that* $\text{Pot}_p(\xi^g - 1) = a + \left[\dfrac{2}{p}\right]$.

Numbers ξ exist such that $\text{Pot}_p(\xi^h - 1) = a + \left[\dfrac{2}{p}\right]$, where $h = \phi(p^a)$. Let $g = s.h$, where p does not divide s. Then since

$$(\xi^g - 1)/(\xi^h - 1) = 1 + \xi^h + \xi^{2h} + \ldots + \xi^{(s-1)h} \equiv s \pmod{p^{a+[2/p]}},$$

we have

$$\mathrm{Pot}_p(\xi^g - 1) = \mathrm{Pot}_p(\xi^h - 1) = \alpha + \left[\frac{2}{p}\right].$$

3. Theorem 1. *If B_k be a balanced m-set, then*

$$2\, G_{2j+1}(B_k) \equiv (k - 2j)\, m\, G_{2j}(B_k) \pmod{m^2 n}$$

where $n = m/2$, only when m is even and k odd; otherwise $n = m$.

We have

$$\prod_{i=1}^{k} (x + b_i) = \prod_{i=1}^{k} (x + m - b_i).$$

Therefore

$$\sum_{r=0}^{k} G_r(B_k)\, x^{k-r} = \sum_{r=0}^{k} (-1)^r G_r(B_k)\, (x + m)^{k-r}.$$

Equating the coefficients of $x^{k-(2j+1)}$, we get

$$2G_{2j+1}(B_k) = \binom{k-2j}{1} m\, G_{2j}(B_k) - \binom{k-2j+1}{2} m^2\, G_{2j-1}(B_k) + \ldots . + \binom{k}{2j+1} m^{2j+1}\, G_0(B_k).$$

Therefore

$$G_{2j+1}(B_k) \equiv 0 \pmod{n}, \quad j = 0, 1, 2, \ldots, \left[\frac{k-1}{2}\right].$$

In particular

$$G_{2j-1}(B_k) \equiv 0 \pmod{n}, \quad j = 1, 2, 3, \ldots, \left[\frac{k+1}{2}\right].$$

Hence the theorem.

Again, if B_k be a balanced m-set, we notice that

$$2S_{2j+1}(B_k) = \sum_{i=1}^{k} \{b_i^{2j+1} + (m - b_i)^{2j+1}\}.$$

Therefore

$$2S_{2j+1}(B_k) \equiv (2j + 1)\, m\, S_{2j}(B_k) \pmod{m^2 t},$$

where $t = m$ or $m/2$, according as m is odd or even.

4. Theorem 2. *If B_k be a self-contained set modulo m, then*

$$G_{2j}(B_k) \equiv 0 \equiv S_{2j}(B_k) \pmod{p^{u-\alpha-[2/p]}};$$

where $\mathrm{Pot}_p\, m = u$, *and* $\mathrm{Piq}_p(2j) = \alpha$; *and* $j > 0$.

Evidently, we can suppose that $\alpha \leqq u - \left[\frac{2}{p}\right]$. Now let ξ be a number such that $\mathrm{Pot}_p(\xi^{2j} - 1) = \alpha + \left[\frac{2}{p}\right]$.

https://doi.org/10.1017/S0013091500008464 Published online by Cambridge University Press

Then $\xi^{2j} G_{2j}(B_k) = G_{2j}(\xi B_k) \equiv G_{2j}(B_k) \pmod{p^u}$,
whence $(\xi^{2j} - 1) G_{2j}(B_k) \equiv 0 \pmod{p^u}$,
and $G_{2j}(B_k) \equiv 0 \pmod{p^{u-a-[2/p]}}$.

As an immediate consequence of Theorem 2, we have

$$(m,\ M_{2j})\, G_{2j}(B_k) \equiv 0 \pmod{m}.$$

The above proof holds good also when G is replaced by S.

5. Theorem 3. *If B_k be a balanced m-set, self-contained modulo m, then*

$$2\,(m,\ M_{2j})\, S_{2j+1}(B_k) \equiv 0 \equiv 2\,(m,\ M_{2j})\, G_{2j+1}(B_k) \pmod{m^2};\ j > 0.$$

This theorem follows directly from theorems 1 and 2.

If $(k, 2j) = g$, then the second part of this theorem takes the form

$$2\,(m,\ M_{2j} N_g / M_g)\, G_{2j+1}(B_k) \equiv 0 \pmod{m^2},$$

for $\mathrm{Pot}_p(k - 2j) \geqq \mathrm{Pot}_p\, g$.

6. When set B_k consists of integers less than and prime to m, Theorem 3 leads to the following generalisation of Leudesdorf's Theorem:

$$2\,(m,\ N_g)\, G_{2j+1}(B_k) \equiv 0 \pmod{m^2};\ j \geqq 1,\ g = (k,\ 2j),\ k = \phi(m).$$

Let C denote the set of integers $1, 2, 3, \ldots, m-1$; and let D denote the set $0, 1, 2, 3, \ldots, m-1$.

Then for $j \geqq 1$, we have

$$2\,(m,\ M_{2j})\, G_{2j+1}(C) \equiv 0 \pmod{m^2},$$

and

$$2\,(m-1,\ M_{2j})\, G_{2j+1}(D) \equiv 0 \pmod{(m-1)^2}.$$

Since $G_{2j+1}(C) = G_{2j+1}(D)$, we get

$$2\,(m.\,(m-1),\ M_{2j})\, G_{2j+1}(C) \equiv 0 \pmod{m^2\,(m-1)^2}.$$

This is a generalisation[1] of two theorems of Glaisher. The theorem holds when G is replaced by S.

In particular, if E denote the set of integers $1, 2, 3, \ldots, p^u - 1$, we have

$$G_{2j+1}(E) \equiv 0 \pmod{p^{2u-\lambda-[2/p]}},$$

where $\lambda = \mathrm{Piq}_p(2j)$, and $j \geqq 1$.

---

[1] J. W. L. Glaisher, *Messenger of Math.*, **28** (1898), 184-185. For another generalisation see H. Gupta, *Proc. Edinburgh Math. Soc.* (2), **4** (1935), 61-66.

GOVERNMENT COLLEGE,
HOSHIARPUR, INDIA.

https://doi.org/10.1017/S0013091500008464 Published online by Cambridge University Press