Congruence Properties of G-Functions

By HANSRAJ GUPTA.

(*Received* 12*th February*, 1934, *and in revised form* 22*nd April*, 1934. *Read* 3*rd March*, 1934.)

§ 1. Denoting the sum of the products of the first n natural numbers taken r at a time by the symbol $G(n, r)$, I have shown[1] that

$$G(n+1, r) = G(n, r) + (n+1)\, G(n, r-1), \tag{1.1}$$

with the initial values $G(n, 0) = 1$; $G(n, r) = 0$, $r > n$; and

$$G(n, n) = n! \tag{1.2}$$

In general it was shown that

$$G(n, r) = \sum_{m=1}^{r} \left\{ f_m(r) \cdot \binom{n+1}{2r-m+1} \right\}, \tag{1.3}$$

where $f_m(r) = (2r - m)\{f_m(r-1) + f_{m-1}(r-1)\}$, $\quad f_0(r) = 0$,

$$f_1(r) = \frac{(2r)!}{2^r . r!}, \text{ and } f_r(r) = r! \tag{1.4}$$

Defining $G(x, r)$ by the fundamental relation:

$$G(x+1, r) = G(x, r) + (x+1)\, G(x, r-1), \tag{1.11}$$

for all values of x, we get

$$G(x, r) = \sum_{m=1}^{r} \left\{ f_m(r) \cdot \binom{x+1}{2r-m+1} \right\}, \qquad r \geqq 1; \tag{1.31}$$

$$= \frac{(r+1)!}{(2r)!} \binom{x+1}{r+1} \cdot \{a_1 x^{r-1} + a_2 x^{r-2} + a_3 x^{r-3} + \dots + a_{r-1} x + a_r\}; \tag{1.5}$$

where the a's are positive or negative integers. (1.6)

§ 2. Consider the series :

$$\phi(n+1) \equiv y^{-n-1} + G(-n-1, 1)\, y^{-n-2} + G(-n-1, 2)\, y^{-n-3} + \dots + G(-n-1, r)\, y^{-n-r-1} + \dots$$

for $y > n$.

---

[1] "Sums of Products of first n natural numbers taken r at a time." *Journal of the Indian Math. Society*, Vol. XIX, Part II, pp. 1-6.

Multiplying both sides by $(y-n)$, we get

$$(y-n)\,\phi\,(n+1)=\sum_{r=0}^{\infty}\{G\,(-n-1,r)-n\,G\,(-n-1,r-1)\}\,y^{-n-r},$$
$$=\sum_{r=0}^{\infty}\{G\,(-n,r)\,y^{-n-r}\}\equiv\phi\,(n).$$

Therefore

$$\phi\,(n+1)=\frac{1}{(y-n)}\,\phi\,(n)=\frac{1}{(y-n)\,(y-n+1)}\,\phi\,(n-1)=\ldots.$$
$$=\left[(n+1)!\binom{y}{n+1}\right]^{-1}\text{ because }\phi\,(1)=y^{-1},\tag{2.1}$$
$$=\frac{(-1)^n}{n!\,y}\left\{\binom{n}{0}-\binom{n}{1}\left(1-\frac{1}{y}\right)^{-1}+\binom{n}{2}\left(1-\frac{2}{y}\right)^{-1}-\ldots.+(-1)^n\binom{n}{n}\left(1-\frac{n}{y}\right)^{-1}\right\}.\tag{2.2}$$

Comparing the coefficients of y^{-n-r-1}, we get

$$n!\;G\,(-n-1,r)=\sum_{k=0}^{n-1}\left\{\binom{n}{k}.(-1)^k.(n-k)^{r+n}\right\},\tag{2.3}$$

or

$$(n-1)!\;G\,(-n-1,r)=\sum_{k=0}^{n-1}\left\{\binom{n-1}{k}.(-1)^k.(n-k)^{r+n-1}\right\}.\tag{2.31}$$

In particular, $G\,(-2,r)=1$; $G\,(-3,r)=2^{r+1}-1$;

$$2!\;\;G\,(-4,r)=3^{r+2}-2.2^{r+2}+1.$$

§ 3. We will now establish some general congruences connected with the G-Functions. In what follows p will denote an odd prime, and i, j, any integers positive, negative or zero.

Consider the product $P\equiv(x+1)(x+2)(x+3)\ldots(x+i)(x+i+1)\ldots(x+i+j)$. Evidently $P\equiv\sum_{r=0}^{i+j}\{G\,(i+j,r)\,x^{i+j-r}\}$. And if $y=x+i$, then

$$P=(y-i+1)\,(y-i+2)\,(y-i+3)\,..\,(y-1)\,y\,.\,(y+1)\ldots(y+j),$$
$$=\{y^i-G(i-1,1)\,y^{i-1}+G(i-1,2)y^{i-2}-\ldots+(-1)^rG(i-1,r)y^{i-r}+\ldots+(-1)^{i-1}G\,(i-1,i-1)y\}$$
$$.\{y^j+G(j,1)\,y^{j-1}+G(j,2)\,y^{j-2}+\ldots+G(j,k)\,y^{j-k}+\ldots+G(j,j)\},$$
$$=\sum_{r=0}^{i+j-1}\{[r]\,y^{i+j-r}\};$$

where

$$[r]=G\,(j,r)-G\,(i-1,1)\,G\,(j,r-1)+\ldots+(-1)^kG\,(i-1,k)\,G(j,r-k)+\ldots+(-1)^rG\,(i-1,r),\text{ and }[0]=1.$$

Comparing the coefficients of the powers of x, we get

$$G(i+j,r)=\binom{i+j}{r}i^r+[1]\binom{i+j-1}{r-1}i^{r-1}+\ldots+[k]\binom{i+j-k}{r-k}i^{r-k}+\ldots+[r]. \quad (3.1)$$

In view of (2.1), this result holds for all integral values of i, j.

I. Putting $i=1$, and $j=p-1$, we have

$$[r]=G(p-1,r).$$

Therefore,

$$G(p,r)=\binom{p}{r}+G(p-1,1).\binom{p-1}{r-1}+G(p-1,2).\binom{p-2}{r-2}+\ldots.$$

$$+G(p-1,r-2).\binom{p-r+2}{2}+G(p-1,r-1).\binom{p-r+1}{1}+G(p-1,r),$$

whence $(r-1)\,G(p-1,r-1)=\binom{p}{r}+G(p-1,1).\binom{p-1}{r-1}+\ldots$

$$+G(p-1,r-2).\binom{p-r+2}{2}. \quad (3.2)$$

Putting $r=2,3,4,\ldots,p-1$ in (3.2) and remembering that $\binom{p}{r}\equiv 0\ (\text{mod. } p)$, $1\leqq r\leqq p-1$, we have

$$G(p-1,k)\equiv 0\ (\text{mod. } p),\ \ k\leqq p-2.$$

This is Lagrange's Theorem.

II. Also putting $r=p$, we have

$$(p-1)\,G(p-1,p-1)\equiv 1\ (\text{mod. } p).$$

Thus $$(p-1)!\equiv -1\ (\text{mod. } p).$$

This is Wilson's Theorem.

III. Putting $i=p$ in (3.1), we have for all integral values of j,

$$G(p+j,r)\equiv G(j,r),\ (\text{mod. } p),\ \ 0<r\leqq p-2; \quad (3.3)$$

and $$\equiv G(j,r)+(-1)^{p-1}G(p-1,p-1)\,G(j,r-p+1),\ (\text{mod. } p),\ \ r\geqq p-1;$$

$$\equiv G(j,r)-G(j,r-p+1),\ (\text{mod. } p),\ \ r\geqq p-1. \quad (3.31)$$

In particular $G(p-2,r)\equiv 1\ (\text{mod. } p)$, $r\leqq p-2$. (3.32)

For $r=p-2$, we get $G(p-2,p-2)\equiv 1\ (\text{mod. } p)$;

or $$(p-2)!\equiv 1\ (\text{mod. } p).$$

Thus (3.3) covers Wilson's Theorem. It covers also Lagrange's Theorem as is seen by putting $j=-1$.

As another remarkable case of (3.3), we have

$$G(p-3,r)\equiv 2^{r+1}-1,\ (\text{mod. } p);\ 0<r\leqq p-2. \quad (3.33)$$

https://doi.org/10.1017/S0013091500007999 Published online by Cambridge University Press

When $r = p - 2$, we get $2^{p-1} \equiv 1 \pmod{p}$, which is a particular case of Fermat's Theorem.

When $0 \leqq j < r$, we have

$$G(p+j, r) \equiv - G(j, r-p+1), \pmod{p}; \tag{3.34}$$

where we take $G(j, -k) = 0$ when j and k are integers $j \geqq 0$, $k > 0$, and $G(0, 0) = 1$.

Putting $i = p$ and $j = -1$ in (3.1),

$$G(p-1, r) \equiv (-1)^r G(p-1, r) \pmod{p^2}, \ 2 \leqq r \leqq p-2.$$

If $r = 2k+1$, we get

$$G(p-1, 2k+1) \equiv 0 \pmod{p^2}, \ 1 \leqq k \leqq \frac{p-3}{2}. \tag{3.35}$$

In particular $G(p-1, p-2) \equiv 0, \pmod{p^2}$, $p \geqq 5$.
This is Wolstenholme's Theorem.

§ 4. Proof of Fermat's Theorem: *If a is prime to p,*

$$a^{\phi(p^u)} \equiv 1 \ (mod.\ p^u),$$

where $\phi(p^u)$ denotes as usual the number of integers less than and prime to p^u.

We have $G(p-j-1, r) \equiv G(-j-1, r) \pmod{p}$, $0 < r \leqq p-2$. Hence

$$\begin{aligned}(j-1)!\ G(-j-1, p-j) &\equiv (j-1)!\ G(p-j-1, p-j) \pmod{p}, \ 2 \leqq j < p; \\ &\equiv 0 \pmod{p}.\end{aligned}$$

Putting $j = 2, 3, 4, \ldots, p-1$ in succession, we get

$$2^{p-1} - 1 \equiv 0 \pmod{p}; \quad \text{therefore } 2^{p-1} \equiv 1 \pmod{p},$$

$$3^{p-1} - \binom{2}{1} 2^{p-1} + 1 \equiv 0 \pmod{p}; \quad \text{hence } 3^{p-1} \equiv 1 \pmod{p}.$$

Let $a^{p-1} \equiv 1 \pmod{p}$, $a = 2, 3, 4, \ldots, i-1$; $i \leqq p-1$. Then $(i-1)!\ G(-i-1, p-i) \equiv 0 \pmod{p}$, so that by (2.3)

$$\begin{aligned}i^{p-1} - \binom{i-1}{1}(i-1)^{p-1} + \binom{i-1}{2}(i-2)^{p-1} - \binom{i-1}{3}(i-3)^{p-1} + \ldots \\ + (-1)^{i-1} \equiv 0 \pmod{p},\end{aligned}$$

or

$$i^{p-1} \equiv \binom{i-1}{1} - \binom{i-1}{2} + \binom{i-1}{3} - \ldots + (-1)^{i-1}\binom{i-1}{i-2} + (-1)^i \equiv 1 \pmod{p}.$$

https://doi.org/10.1017/S0013091500007999 Published online by Cambridge University Press

Hence by inductive reasoning, we have

$$a^{p-1} \equiv 1 \pmod{p}, \quad a < p.$$

For values of $a > p$ and prime to it, we have

$$a^{p-1} \equiv a'^{p-1} \equiv 1 \pmod{p} \text{ where } a \equiv a' \pmod{p}, \quad a' < p.$$

This proves the theorem when $u = 1$.

When $u > 1$, we have

$$\begin{aligned} a^{\phi(p^u)} &\equiv a^{p^{u-1}(p-1)} \equiv (a^{p-1})^{p^{u-1}}, \\ &\equiv (kp+1)^{p^{u-1}}, \text{ since } (a, p) = 1, \\ &\equiv 1 \pmod{p^u}, \text{ for } \binom{p^{u-1}}{r} \equiv 0 \pmod{p^{u-1-\alpha}}[1] \end{aligned}$$

where $r \equiv 0 \pmod{p^\alpha}$ and $\not\equiv 0 \pmod{p^{\alpha+1}}$.

In general if $(a, n) = 1$,

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

For if $n = p_1^\alpha p_2^\beta p_3^\gamma \ldots . p_i^k \ldots . p_n^u = \Pi(p_i^k)$,

then $\quad a^{\phi(n)} \equiv a^{h\phi(p_i^k)} \equiv 1 \pmod{p_i^k}$, $h = \phi(p_1^\alpha) \cdot \phi(p_2^\beta) \ldots . \phi(p_n^u)/\phi(p_i^k)$.

§ 5. THEOREM. *The a's in* (1.5) *are each* $\equiv 0$ (*mod.* p), *where* $r + 1 < p < 2r$.

Proof. Because $r \leqq p-2$, we have $G(p+j, r) \equiv 0 \pmod{p}$, $-1 \leqq j \leqq r-1$. Therefore $(2r)!\ G(p+j, r) \equiv 0 \pmod{p^2}$;

$$\text{or } (r+1)! \binom{p+j+1}{r+1} \{a_1(p+j)^{r-1} + a_2(p+j)^{r-2} + a_3(p+j)^{r-3} + \ldots + a_r\} \equiv 0 \pmod{p^2}.$$

Since $\quad (r+1)! \binom{p+j+1}{r+1} \equiv 0 \pmod{p}$, and $\not\equiv 0 \pmod{p^2}$; when $-1 \leqq j \leqq r-1$, we must have $a_1 j^{r-1} + a_2 j^{r-2} + a_3 j^{r-3} + \ldots . + a_{r-1} j + a_r \equiv 0 \pmod{p}$, for $j = -1, 0, 1, 2, \ldots ., r-1$.

r being $\leqq p-2$, this congruence has more than $(r-1)$ incongruent roots, therefore $a_k \equiv 0 \pmod{p}$, $\quad 1 \leqq k \leqq r$.

§ 6. THEOREM. *In* [1.3], $f_m(r) \equiv 0$ (*mod.* p), $m = 1, 2, 3, \ldots ., 2r-p+1$; *where* $\quad r + 1 < p < 2r$.

Let $p = 2k - 1$, then

$$\begin{aligned} G(p-1, k) &\equiv f_1(k)\binom{p}{2k} + f_2(k)\binom{p}{2k-1} + \ldots . + f_k(k)\binom{p}{k+1}, \\ &\equiv f_2(k), \pmod{p}. \end{aligned}$$

[1] Lemma 1 in my paper on "A Theorem of Gauss," to be published in the next number of these *Proceedings*.

But $G(p-1, k) \equiv 0 \pmod{p}$, for $k < p-1$;

hence $f_2(k) \equiv 0 \pmod{p}$.

Also $f_1(k) \equiv 1.3.5. \ldots . (2k-1) \equiv 0 \pmod{p}$.

Thus the theorem holds when $r = k = \dfrac{p+1}{2}$.

Suppose the theorem holds when $k \leqq r \leqq t-1 < p-2$,

so that $f_s(t-1) \equiv 0 \pmod{p}$, $s = 1, 2, 3, \ldots, 2t-p-1$.

Since $f_l(t) = (2t-l)\{f_l(t-1) + f_{-}\ (t-1)\}$,

$f_l(t) \equiv 0 \pmod{p}$, $l = 1, 2, 3, \ldots, 2t-p-1$.

Also when $l = 2t-p$, $2t-l \equiv 0 \pmod{p}$, therefore $f_{\ -p}(t) \equiv 0 \pmod{p}$.

Again $t \leqq p-2$, so that $G(p-1, t) \equiv 0 \pmod{p}$.

But $G(p-1, t) \equiv f_{2t-p+1}(t) \pmod{p}$, therefore $f_{2t-p+1}(t) \equiv 0 \pmod{p}$.

Thus $f_l(t) \equiv 0 \pmod{p}$, $l = 1, 2, 3, \ldots, 2t-p+1$.

The theorem is now proved by induction.

For $r \geqq p-1$, we can prove that $f_m(r) \equiv 0 \pmod{p}$ $m = 1, 2, 3, \ldots, p-2$.

§ 7. THEOREM. *For odd values of $r \geqq 3$,*

$$(2r)!\ G(j, r) \equiv 0 \ (mod.\ j^2(j+1)^2).$$

We have

$$(2r)!\ G(j, r) = (r+1)! \binom{j+1}{r+1} \{a_1 j^{r-1} + a_2 j^{r-2} + a_3 j^{r-3} + \ldots + a_r\}.$$

Let p be an "odd prime" $> | a_1 - a_2 + a_3 - a_4 + \ldots + a_r |$, also $> 2r$ and $|a_r|$.

Then $G(p-1, r) \equiv 0 \pmod{p^2}$, so that

$$a\ \ - a_2 + a_3 - a_4 + \ldots + a_r \equiv 0 \pmod{p}.$$

This can only be if $a_1 - a_2 + a_3 - a_4 + \ldots + a_r = 0$.

Hence $(j+1)$ must be a factor of $a_1 j^{r-1} + a_2 j^{r-2} + a_3 j^{r-3} + \ldots + a_r$.

This proves the theorem so far as $(j+1)^2$ is concerned.

Again $G(p, r) = G(p-1, r) + p\,G(p-1, r-1)$,

$\equiv 0 \pmod{p^2}$.

Therefore $a_r \equiv 0$ (mod, p), for which it is necessary that

$a_r = 0$.

This proves the theorem completely.

https://doi.org/10.1017/S0013091500007999 Published online by Cambridge University Press