ON A GENERALIZATION OF THE WILSON-GLAISHER THEOREM

BY GIOVANNI RICCI

1. *Introduction.* J. W. L. Glaisher* has shown that, if n be any number, p any odd prime not exceeding n, k the integral part of the quotient n/p, and if A_r denote the sum of the products of the first $n-1$ consecutive integers taken r together, then

$$A_{p-1} + k \equiv 0 \pmod{p}.$$

This theorem contains Wilson's theorem as the special case $n=p$, and it has been extended by R. E. Moritz† in the following form. If $n=kp+q$, p an odd prime, $0 \leqq q < p$, and if ${}^mA_r$ denote the sum of the products of any $n-1$ consecutive numbers, $m+1$, $m+2$, $\cdots$, $m+n-1$ taken r together; if $0<q<p$, then ${}^mA_{p-1}+k\equiv 0$, (mod p). If $q=0$, then ${}^mA_{p-1}+k\equiv 0$, or $\equiv 1$, (mod p), according as m is, or is not, a multiple of p.

It is the purpose of the present paper to show that the Wilson-Glaisher theorem, the Moritz theorem, and other theorems are special cases of a still more general theorem relating to the symmetric functions of special systems of numbers, these systems being composed of the residues of powers, eventually repeated, for different moduli.

2. *The Generalized Theorem.* We shall prove the following general theorem.

Let $m=p^\alpha q^\beta \cdots r^\gamma$, ($p, q, \cdots, r$ odd primes, $p<q< \cdots <r$; $\alpha \geqq 1, \beta \geqq 1, \cdots, \gamma \geqq 1$), be an odd number and let $\rho, \sigma, \cdots, \chi$ be any divisors respectively of $\phi(p^\alpha)$, $\phi(q^\beta)$, $\cdots$, $\phi(r^\gamma)$, where $\phi(n)$ denotes Euler's Indicator; we shall write $\rho = p^a\lambda$ (λ divisor

* J. W. L. Glaisher, *Congruences relating to the sums of products of the first n numbers and to other sums of products*, Quarterly Journal of Mathematics, vol. 31 (1900), pp. 1–35; see p. 23. See also L. E. Dickson, *History of the Theory of Numbers*, vol. I, p. 99.

† R. E. Moritz, *On an extension of Glaisher's generalization of Wilson's theorem*, Tôhoku Mathematical Journal, vol. 28 (1927), p. 198–201.

of $p-1$), $\sigma=q^b\mu$ (μ divisor of $q-1$), $\cdots$, $\chi=r^c\nu$ (ν divisor of $r-1$). Let $(u_0, u_1, \cdots, u_{\rho-1}), (v_0, v_1, \cdots, v_{\rho-1}), \cdots, (w_0, w_1, \cdots, w_{\chi-1})$ be the complete root systems respectively of the congruences

$$u^\rho \equiv 1 \pmod{p^\alpha}; \quad v^\sigma \equiv 1 \pmod{q^\beta}; \quad \cdots; \quad w^\chi \equiv 1 \pmod{r^\gamma}.$$

Consider the $\tau=\rho\sigma\cdots\chi$ numbers

$$t_1, t_2, \cdots, t_\tau$$

two by two incongruent (mod m), represented by the form

$$Au_d + Bv_e + \cdots + Cw_f,$$

$$(0 \leqq d \leqq \rho - 1, 0 \leqq e \leqq \sigma - 1, \cdots, 0 \leqq f \leqq \chi - 1),$$

in which $A, B, \cdots, C$ denote auxiliary integers satisfying the congruences

$$A \equiv 1 \pmod{p^\alpha}; \qquad B \equiv 1 \pmod{q^\beta}; \qquad \cdots; \qquad C \equiv 1 \pmod{r^\gamma};$$

$$A \equiv 0\left(\operatorname{mod} \frac{m}{p^\alpha}\right); \quad B \equiv 0\left(\operatorname{mod} \frac{m}{q^\beta}\right); \quad \cdots; \quad C \equiv 0\left(\operatorname{mod} \frac{m}{r^\gamma}\right).$$

Consider the $k\tau$ integers $t_{j,i}$, ($j=1, 2, \cdots, \tau$; $i=1, 2, \cdots, k$), k by k congruent (mod m), precisely,

(1) $\quad t_{j,i} \equiv t_j \pmod{m}, \quad (i = 1, 2, \cdots, k), \quad j = 1, 2, \cdots, \tau,$

and h other *arbitrary* integers

(2) $\quad z_1, z_2, \cdots, z_h, \qquad (h \geqq 0).$

If $R_{s\tau}(m; \rho, \sigma, \cdots, \chi \| k, h)$ denotes the sum of the products of integers (1) *and* (2) *taken $s\tau$ together,* ($R_0=1$), *then from any one of the inequalities*

$$h < \lambda, h < \mu, \cdots, h < \nu$$

there follows the corresponding congruence

$$
\text{(A)}\quad R_{s\tau}(m;\,\rho,\,\sigma,\,\cdots,\,\chi\|k,\,h)\begin{cases}\equiv(-1)^{s\tau(\lambda-1)/\lambda}\begin{pmatrix}\dfrac{k\tau}{\lambda}\\ \dfrac{s\tau}{\lambda}\end{pmatrix}\pmod{p^{\alpha}},\\[2ex] \equiv(-1)^{s\tau(\mu-1)/\mu}\begin{pmatrix}\dfrac{k\tau}{\mu}\\ \dfrac{s\tau}{\mu}\end{pmatrix}\pmod{q^{\beta}},\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ \equiv(-1)^{s\tau(\nu-1)/\nu}\begin{pmatrix}\dfrac{k\tau}{\nu}\\ \dfrac{s\tau}{\nu}\end{pmatrix}\pmod{r^{\gamma}}.\end{cases}
$$

In the special case $s=k$, $h<\lambda$, $h<\mu$, $\cdots$, $h<\nu$, if the integers

$$
\frac{k\tau}{\lambda}(\lambda-1),\quad \frac{k\tau}{\mu}(\mu-1),\cdots,\frac{k\tau}{\nu}(\nu-1)
$$

are all even or all odd, we have the congruence

$$
R_{k\tau}(m;\,\rho,\,\sigma,\,\cdots,\,\chi\|k,\,h)\equiv\pm 1\pmod{m}.
$$

3. *Special Cases.* We observe that the $\phi(m)$ integers (mod m), prime to m, are characterized by their satisfying the congruences

$$
t^{\phi(p^{\alpha})}\equiv 1\pmod{p^{\alpha}};\quad t^{\phi(q^{\beta})}\equiv 1\pmod{q^{\beta}};\quad\cdots;\quad t^{\phi(r^{\gamma})}\equiv 1\pmod{r^{\gamma}}.
$$

Therefore we may express Wilson's classic theorem and its generalizations by means of the forms

$$
\begin{aligned}
&R_{p-1}(p;p-1\|1,0) &&\equiv -1\pmod{p} &&\text{(Wilson)*},\\
&R_{\phi(p^{\alpha})}(p^{\alpha};\phi(p^{\alpha})\|1,0) &&\equiv -1\pmod{p^{\alpha}} &&\Big\}\ \text{(Gauss)†},\\
&R_{\phi(m)}(m;\phi(p^{\alpha}),\phi(q^{\beta}),\cdots,\phi(r^{\gamma})\|1,0) &&\equiv 1\pmod{m} &&\\
&R_{p-1}(p;\,p-1\|k,\,h) &&\equiv -k\pmod{p} &&\text{Glaisher–Moritz‡},
\end{aligned}
$$

* See L. E. Dickson, op. cit., p. 62.

† See L. E. Dickson, op. cit., p. 65.

‡ See L. E. Dickson, op. cit., p. 99; and R. E. Moritz, loc. cit.

$$R_{s\tau}(m;\phi(p^\alpha),\phi(q^\beta),\cdots,\phi(r^\gamma)\|k,0) \quad (\tau=\phi(m)=\phi(p^\alpha)\cdots\phi(r^\gamma)) \quad \text{(M. BAUER)*} \quad \begin{cases} \equiv(-1)^{s\tau/(p-1)}\begin{pmatrix}\frac{k\tau}{p-1}\\ \frac{s\tau}{p-1}\end{pmatrix} \pmod{p^\alpha}, \\ \equiv(-1)^{s\tau/(q-1)}\begin{pmatrix}\frac{k\tau}{q-1}\\ \frac{s\tau}{q-1}\end{pmatrix} \pmod{q^\beta}, \\ \cdots\cdots\cdots\cdots\cdots \\ \equiv(-1)^{s\tau/(r-1)}\begin{pmatrix}\frac{k\tau}{r-1}\\ \frac{s\tau}{r-1}\end{pmatrix} \pmod{r^\gamma}. \end{cases}$$

For the ω-ic residues (mod p^α),

$$R_\rho(p^\alpha;\rho\|1,0)\equiv(-1)^{\rho-1} \pmod{p^\alpha};\qquad \rho=\frac{\phi(p^\alpha)}{D(\omega,\phi(p^\alpha))}\dagger.$$

And also

$$(3)\quad R_{s\lambda}(m;\rho,\sigma,\cdots,\chi\|1,0)\equiv(-1)^{s(\lambda-1)}\begin{pmatrix}\frac{\tau}{\lambda}\\ s\end{pmatrix}, \pmod{p^\alpha}, \quad \text{(RICCI).}\ddagger$$

4. PROOF. Let $R_{n_i}(m;\rho,\sigma,\cdots,\chi\|1,0)$ denote the sum of the products of the τ numbers $t_{j,i}$, $(j=1,2,\cdots,\tau)$, of the system (1) taken n_i together, and let R_n' be the sum of the products of the h numbers $z_1,z_2,\cdots,z_h$ taken n together ($R_n'=1$, if $hn=0$). Obviously we have the equality

$$(4)\quad R_{s\tau}(m;\rho,\sigma,\cdots,\chi\|k,h) = \sum\left\{\prod_{i=1}^{k}R_{n_i}(m;\rho,\sigma,\cdots,\chi\|1,0)\right\}R_n',$$

* See L. E. Dickson, op. cit., p. 88. (Bauer [186].)

† See P. Bachmann, *Niedere Zahlentheorie*, Teil I, Leipzig, 1902, p. 347.

‡ See G. Ricci, *Sulle funzioni simmetriche delle radici dell'unità secondo un modulo composto*, Annali di Matematica, (4), vol. 9 (1931), p. 190, formula (B_4).

in which the sum is extended to the solutions in integers $\geqq 0$ of the equation

$$n_1 + n_2 + \cdots + n_k + n = s\tau,$$
$$(0 \leqq n_i \leqq \tau,\ i = 1, 2, \cdots, k;\ 0 \leqq n \leqq h).$$

If $n_i \not\equiv 0 \pmod{\lambda}$, then it is known* that

$$R_{n_i}(m;\rho,\sigma,\cdots,\chi\|1,0) \equiv 0 \pmod{p^\alpha},$$

and if $n_i = s\lambda$, then the congruence (3) stands. Therefore if one at least of the integers $n_1, n_2, \cdots, n_k$ is $\not\equiv 0 \pmod{\lambda}$, then the corresponding term on the right of (4) is divisible by p^α; hence, for the relation $0 \leqq n \leqq h < \lambda$, we obtain

$$R_{s\tau}(m;\rho,\sigma,\cdots,\chi\|k,h)$$
$$\equiv \sum \prod_{i=1}^{k} R_{s_i\lambda}(m;\rho,\sigma,\cdots,\chi\|1,0) \pmod{p^\alpha},$$
$$\left(s_1 + s_2 + \cdots + s_k = s\frac{\tau}{\lambda};\ 0 \leqq s_i \leqq \frac{\tau}{\lambda}\right).$$

Then, by (3), we may write

$$R_{s\tau}(m;\rho,\sigma,\cdots,\chi\|k,h) \equiv (-1)^{s\tau(\lambda-1)/\lambda} \sum \prod_{i=1}^{k} \binom{\frac{\tau}{\lambda}}{s_i} \pmod{p^\alpha},$$
$$\left(s_1 + s_2 + \cdots + s_k = \frac{s\tau}{\lambda}\right);$$

and, by a well known formula on binomial coefficients, from this congruence we deduce the first formula of (A). We may deduce the other formulas in a similar manner.

R. Scuola Normale Superiore
Pisa, Italy

* See G. Ricci, loc. cit., formula (B_4).