ON AN ARITHMETICAL THEOREM CONNECTED WITH ROOTS OF UNITY, AND ITS APPLICATION TO GROUP-CHARACTERISTICS*

By W. BURNSIDE.

[Communicated February 12th, 1903.—Received February 20th, 1903.]

I.

The arithmetical theorem in question may be stated as follows :—

Let ω be a primitive m-th root of unity, χ a rational integral function of ω with real integers as coefficients, and χ' the conjugate imaginary of χ. Let $S\ (= \Sigma\chi\chi')$ be formed by taking for ω each of the $\phi(m)$ distinct primitive m-th roots of unity in turn, constructing the product $\chi\chi'$, and adding the $\phi(m)$ products so obtained. Then the absolutely least value of S, other than zero, is $\phi(m)$.

The case in which m is the power of a prime, say p^a, will be first onsidered.

Since ω is the root of an irreducible equation of degree $\phi(m)$, with unity for the leading coefficient, χ can be expressed as a rational integral function of ω, of degree not exceeding $\phi(m)-1$, with integral coefficients. Hence

$$\chi = a_0+a_1\omega+a_2\omega^2+\ldots+a_{\phi(m)-1}\omega^{\phi(m)-1}.$$

Since χ and χ' are conjugate imaginaries, $\chi\chi'$ must be positive or zero, and S can only be zero when χ is zero. Now

$$\chi\chi' = \sum_{i=0}^{i=\phi(m)-1} a_i^2+\sum_{i,j} a_i a_j(\omega^{i-j}+\omega^{j-i}),$$

and therefore $$S = \Sigma\chi\chi' = s_0 \sum_{i=0}^{i=\phi(m)-1} a_i^2+2\sum_{i,j} s_{i-j}a_i a_j,$$

where $s_0 = \phi(m) =$ sum of the m-th powers of the primitive m-th roots, $s_{i-j} =$ sum of the $(i-j)$-th powers of the primitive m-th roots, and the latter sum in the expression for S is taken for each distinct pair of suffixes i and j.

---

* [The proof of the theorem in Section I. originally given was incomplete; it has been replaced by that now printed.—*October 17th*, 1903.]

Unless $i-j$ is a multiple of m/p, or $p^{\alpha-1}$, s_{i-j} is zero; and, when $i-j$ is a multiple of $p^{\alpha-1}$, s_{i-j} is equal to $-p^{\alpha-1}$, *i.e.*, $-s_0/(p-1)$. Hence the product $a_i a_j$ will occur in S only when i and j differ by a multiple of $p^{\alpha-1}$. The a's may therefore be divided into $s_0/(p-1)$ sets of $p-1$ each, so that no product term occurs except among the a's belonging to the same set. Any such set will have suffixes

$$i+x\frac{s_0}{p-1} \quad (x = 0, 1, \ldots, p-2),$$

while the values $i = 0, 1, \ldots, \frac{s_0}{p-1}-1$ give the different sets.

The part of S which arises from the first set will be

$$S_0 = \frac{s_0}{p-1}\left[(p-1)\sum_x a^2_{xp^{\alpha-1}} - 2\sum_{x,y} a_{xp^{\alpha-1}} a_{yp^{\alpha-1}}\right]. \qquad \text{(i)}$$

From this the part of S which arises from the i-th set will be given by increasing each suffix by $i-1$.

Equation (i) may be written

$$S_0 = \frac{s_0}{p-1}\left[\sum_x a^2_{xp^{\alpha-1}} + \sum_{x,y} (a_{xp^{\alpha-1}} - a_{yp^{\alpha-1}})^2\right].$$

Since each of the $p-1$ a's is an integer or zero, it is quite obvious that the number in the square brackets cannot be less than $p-1$, unless it is zero. Hence S_0, if not zero, is at least equal to s_0. The same is true of the part of S which arises from any other set of a's; and therefore S itself, if not zero, must be equal to or greater than s_0.

It will now be assumed that the theorem has been proved when m has not more than $n-1$ different prime factors. Suppose then that

$$m = p^\alpha q,$$

where q is the product of powers of $n-1$ distinct primes, and let ω be a primitive p^α-th root of unity and ω' a primitive q-th root of unity; so that $\omega\omega'$ is a primitive m-th root of unity. Here χ may be expressed in the form

$$\chi = \psi_0 + \omega\psi_1 + \omega^2\psi_2 + \ldots + \omega^{p^{\alpha-1}(p-1)-1}\psi_{p^{\alpha-1}(p-1)-1},$$

where each ψ is a rational function of ω' with integral coefficients. Also

$$\chi\chi' = \sum_i \psi_i\psi'_i + \sum_{i,j} (\omega^{i-j}\psi_i\psi'_j + \omega^{j-i}\psi'_i\psi_j).$$

From this expression S is obtained by summing, after replacing ω by each primitive p^α-th root of unity and ω' by each primitive q-th root.

Let Σ denote the partial sum, when ω is replaced by each primitive p^α-th root of unity. Then from the previous case

$$\Sigma = p^{\alpha-1}(p-1)\sum_i \psi_i\psi'_i - p^{\alpha-1}\sum_{i,j}(\psi_i\psi'_j+\psi'_i\psi_j),$$

where in the second term on the right-hand side only those products occur in which i and j differ by a multiple of $p^{\alpha-1}$. Hence Σ can be expressed as the sum of $p^{\alpha-1}$ parts, of which the leading part is given by

$$\Sigma_0 = p^{\alpha-1}(p-1)\sum_x \psi_{xp^{\alpha-1}}\psi'_{xp^{\alpha-1}} - p^{\alpha-1}\sum_{x,y}(\psi_{xp^{\alpha-1}}\psi'_{yp^{\alpha-1}} - \psi'_{xp^{\alpha-1}}\psi_{yp^{\alpha-1}})$$

$$= p^{\alpha-1}\Big[\sum_x \psi_{xp^{\alpha-1}}\psi'_{xp^{\alpha-1}} + \sum_{x,y}(\psi_{xp^{\alpha-1}}-\psi_{yp^{\alpha-1}})(\psi'_{xp^{\alpha-1}}-\psi'_{yp^{\alpha-1}})\Big],$$

while the other parts are obtained by increasing each suffix by the same number.

The part of S which arises from Σ_0, say S_0, is obtained by summing when ω' is replaced in turn by each primitive q-th root of unity. For each ψ that occurs, $\Sigma\psi\psi'$, if not zero, is not less than $\phi(q)$. Now, exactly as before, it is clear that, of the $\frac{1}{2}p(p-1)$ products in the square brackets of the last equation, at least $p-1$ must be different from zero, unless all are zero. Hence, if S_0 is not zero, it cannot be less than $p^{\alpha-1}(p-1)\phi(q)$, *i.e.*, than $\phi(m)$. The same is true for the part of S which arises from each part of Σ. Hence S, if greater than zero, is not less than $\phi(m)$; and the theorem is true when m has n distinct prime factors, if it is true when m has $n-1$. The theorem is therefore completely proved.

The quantity S_0 can be represented in a remarkable form, which is perhaps worth reproducing. It is given here for the case

$$m = p^\alpha q^\beta r^\gamma,$$

which immediately suggests the form in the general case. S_0 is a quadratic function of $(p-1)(q-1)(r-1)$ a's. If these are

$$a_{ijk} \quad (1 \leqslant i \leqslant p-1,\ 1 \leqslant j \leqslant q-1,\ 1 \leqslant k \leqslant r-1),$$

then $S_0/p^{\alpha-1}q^{\beta-1}r^{\gamma-1}$

$$= pqr\sum_{ijk} a_{ijk}^2 - qr\sum_{ik}\Big(\sum_i a_{ijk}\Big)^2 - rp\sum_{jk}\Big(\sum_j a_{ijk}\Big)^2 - pq\sum_{ij}\Big(\sum_k a_{ijk}\Big)^2 + p\sum_i\Big(\sum_{jk} a_{ijk}\Big)^2$$

$$+ q\sum_j\Big(\sum_{ik} a_{ijk}\Big)^2 + r\sum_k\Big(\sum_{ij} a_{ijk}\Big)^2 - \Big(\sum_{ijk} a_{ijk}\Big)^2.$$

II.

Let S be any operation of order m belonging to a group G of finite order N. The $\phi(m)$ powers of S of order m will in general belong to a number of different conjugate sets. If t and no more belong to one set, t must be a factor of $\phi(m)$, and the powers of S will be distributed among $\phi(m)/t, = t'$, distinct conjugate sets, each of which will contain t of them, while the number of conjugate operations, h, in each of the sets is the same. Suppose that in an irreducible representation of G the characteristic of S is χ_1. If n is the number of symbols in the representation, χ_1 is the sum of n m-th roots of unity; and, if S^x is conjugate to S, χ_1 is unaltered when ω, the primitive m-th root of unity in terms of which it is expressed, is replaced by ω^x. If, on the other hand, S^y, where y is relatively prime to m, is not conjugate to S, then, when ω is replaced by ω^y, χ_1 becomes the characteristic of the conjugate set to which S^y belongs. Hence, if $\chi_1, \chi_2, \ldots, \chi_{t'}$ are the characteristics of the t' conjugate sets to which S and its powers of order m belong, then, when ω is replaced in turn by each of the primitive m-th roots of unity, χ_1 takes each of the values $\chi_1, \chi_2, \ldots, \chi_{t'}$ t times. Therefore

$$\chi_1\chi_1'+\chi_2\chi_2'+\ldots+\chi_{t'}\chi_{t'}' = \frac{1}{t}\Sigma\chi\chi',$$

where $\Sigma\chi\chi'$ is the sum for all primitive m-th roots of unity. But $\Sigma\chi\chi'$ is either zero or not less than $\phi(m)(= tt')$. Hence $h(\chi_1\chi_1'+\chi_2\chi_2'+\ldots+\chi_{t'}\chi_{t'}')$. if not zero, is not less than ht'.

Now $\Sigma h\chi\chi' = N$, where the sum is extended to all conjugate sets of G, and $\Sigma h = N$; moreover, for the identical operation $\chi\chi'$ is n^2, Therefore, if $n > 1$, for at least one conjugate set $\chi\chi'$, and therefore χ itself, must be zero. Hence:—

In any irreducible group of linear substitutions of finite order, other than a cyclical group in a single variable, at least one of the characteristics is zero.

To this property of group-characteristics I hope to return on another occasion. It may be here pointed out that, in general, it considerably facilitates the calculation of the characteristics for any given group. As an example the table of characteristics of the simple group of order 504 is given with a short indication of the manner in which it has been arrived at.

The group, which may be represented as a triply-transitive group of degree 9 and class 7, contains the identical operation, represented by S_1;

63 operations of order 2, forming the set S_2; 56 operations of order 3, forming the set S_3; 3·72 operations of order 7, forming the sets S_7', S_7'', S_7'''; 3·56 operations of order 9, forming the sets S_9', S_9'', S_9'''.

For any irreducible representation, χ_2 and χ_3 are rational, as also are $\Sigma\chi_7\chi_7'$, for the three sets of order 7 and $\Sigma\chi_9\chi_9'$ for the three sets of order 9; and, except for the set in which each characteristic is unity, one of these four quantities must vanish. Further $\Sigma h\chi\chi' = 504$ and $\Sigma h\chi = 0$.

If, for instance, χ_7 vanishes, χ_1 must be a multiple of 7. Taking then as a first trial $\chi_1 = 7$,

$$9\chi_2^2+8(\chi_3^2+\Sigma\chi_9\chi_9') = 65, \quad 9\chi_2+8(\chi_3+\Sigma\chi_9) = -1,$$

and the only possible solutions of these, subject to the above conditions, are

$$\chi_2 = -1, \ \chi_3 = -2, \ \chi_9 = 1, \quad \text{or} \quad \chi_2 = -1, \ \chi_3 = 1, \ \chi_9 = -\beta-\beta^{-1},$$

where β is a primitive ninth root of unity. If α represents a primitive seventh root of the unity, the complete table is that given below; and the check on its accuracy is that it satisfies the complete system of relations* that a set of group-characteristics must in any case obey.

	G_1	G_7	G_7'	G_7''	G_7'''	G_8	G_9'	G_9''	G_9'''	h
S_1	1	7	7	7	7	8	9	9	9	1
S_2	1	−1	−1	−1	−1	0	1	1	1	63
S_3	1	−2	1	1	1	−1	0	0	0	56
S_7'	1	0	0	0	0	1	$\alpha+\alpha^{-1}$	$\alpha^2+\alpha^{-2}$	$\alpha^4+\alpha^{-4}$	72
S_7''	1	0	0	0	0	1	$\alpha^2+\alpha^{-2}$	$\alpha^4+\alpha^{-4}$	$\alpha+\alpha^{-1}$	72
S_7'''	1	0	0	0	0	1	$\alpha^4+\alpha^{-4}$	$\alpha+\alpha^{-1}$	$\alpha^2+\alpha^{-2}$	72
S_9'	1	1	$-\beta-\beta^{-1}$	$-\beta^2-\beta^{-2}$	$-\beta^4-\beta^{-4}$	−1	0	0	0	56
S_9''	1	1	$-\beta^2-\beta^{-2}$	$-\beta^4-\beta^{-4}$	$-\beta-\beta^{-1}$	−1	0	0	0	56
S_9'''	1	1	$-\beta^4-\beta^{-4}$	$-\beta-\beta^{-1}$	$-\beta^2-\beta^{-2}$	−1	0	0	0	56

* "Group-Characteristics," *Proc. Lond. Math. Soc.*, Vol. XXXIII., p. 154.