NOTE ON FUNCTIONS PROPER TO REPRESENT A SUBSTITUTION OF A PRIME NUMBER OF LETTERS.

By Prof. *L. J. Rogers.*

§ 1. In order that a rational integral algebraic function $f(z)$ should represent a substitution of p letters, it is sufficient and necessary that the p quantities $f(0), f(1), \ldots f(p-1)$ should be congruent non-respectively to $0, 1, 2 \ldots (p-1)$ for the modulus p.

Starting with this condition, it has been proved by Hermite (see Serret's *Alg.*, § 476) that if $f(z)$ possesses this property for a prime modulus p, then when $\{f(z)\}, \{f(z)\}^2, \ldots, \{f(z)\}^{p-2}$ are expanded, and reduced by Fermat's theorem to functions of degree $(p-1)$, the several coefficients of z^{p-1} are congruent to zero. He also proves that the converse is true, namely, that $f(z)$ will represent a substitution provided these $(p-2)$ coefficients are zero. Now I wish to prove that although these $(p-2)$ conditions are sufficient, yet they are not altogether necessary, inasmuch as they are not all independent.

Let $$z^p + p_1 z^{p-1} + p_2 z^{p-2} + \ldots p_{n-1} z + p_n \equiv 0 \quad \ldots\ldots(1)$$

be a congruence whose roots are $f(0), f(1), \ldots, f(p-1)$, for the modulus p. Without loss of generality we may assume that $f(0) \equiv 0$, so that we may say that $p_n \equiv 0$.

It is easy to see that Hermite's conditions are none other than that the several sums of powers of the roots of the congruence (1) should be zero.

Now it is important to remember that all the roots of (1) are essentially real, so that by Fermat's theorem, $s_{n-r-1} \equiv s_r$ for all values of r.

Theorem. If a congruence have all its roots real, for prime modulus p, then if

$$s_1 \equiv 0 \equiv s_2 \equiv s_3 \equiv \ldots s_{\frac{1}{2}(p-1)},$$

so also will $$s_{\frac{1}{2}(p+1)} \equiv 0 \equiv s_{\frac{1}{2}(p+3)} \ldots \equiv s_{p-2},$$

so that Hermite's conditions will hold good.

We have, by Newton's rule,

$$\begin{aligned} s_1 + p_1 &\equiv 0, \text{ so that } p_1 \equiv 0, \\ s_2 + 2p_2 &\equiv 0, \text{ so that } p_2 \equiv 0, \ldots\ldots\ldots\ldots\ldots(2) \\ s_3 + 3p_3 &\equiv 0, \text{ so that } p_3 \equiv 0, \text{ etc.} \end{aligned}$$

Thus evidently all the coefficients in the equation as far as $p_{\frac{1}{2}(p-1)}$ are zero, while (putting $p = 2m+1$)

$$\left.\begin{aligned} &s_{m+1} + (m+1)\,p_{m+1} \equiv 0, \\ &s_{m+2} + (m+2)\,p_{m+2} \equiv 0, \text{ \&c.,} \\ \text{and } &s_{p-1} \equiv -(p-1)\,p_{p-1} \equiv p_{p-1} \end{aligned}\right\} \quad \ldots\ldots(3).$$

Moreover, by Fermat's theorem and Newton's,

$$p_1 s_{p-1} + p_2 s_{p-2} + \ldots + p_m s_{m+1} + p_{m+1} s_m + \ldots + s_1 p_{p-1} \equiv -s_p \equiv -s_1 \equiv 0,$$

as is obvious identically.

But we also have

$$p_1 s_p + p_2 s_{p-1} + \ldots + p_{m+1} s_{m+1} + \ldots + s_2 p_{p-1} \equiv -s_{p+1} \equiv s_2 \equiv 0,$$

whence $$p_{m+1} s_{m+1} \equiv 0,$$

so that $$s^2_{m+1} \equiv 0 \text{ by (3).}$$

Similarly $$p_1 s_{p+2} + \ldots + p_{m+2} s_{m+2} + \ldots + s_4 p_{p-1} \equiv -s_{p+3} \equiv -s_4 \equiv 0,$$

therefore $$p_{m+2} s_{m+2} \equiv 0 \text{ and } s_{m+2} \equiv 0.$$

Proceeding in this way we easily see that

$$s_{m+1} \equiv 0 \equiv s_{m+2} \equiv s_{m+3} \cdots \equiv s_{p-2},$$

while $$p_1 s_{2p-3} + p_2 s_{2p-4} + \ldots + p_{p-1} s_{p-1} \equiv -s_{2p-2} \equiv -s_{p-1},$$

whence $$p_{p-1} s_{p-1} \equiv -s_{p-1},$$

or by (3),

$$(s_{p-1} + 1)\, s_{p-1} \equiv 0.$$

Now if $s_{p-1} \equiv 0$ the congruence (1) reduces to $z^p \equiv 0$, a case we may lay aside as out of the question, while $s_{p-1} \equiv -1$ gives $p_{p-1} \equiv -1$ and (1) reduces to $z^p - z \equiv 0$, as it ought to do. Hence, it is sufficient in testing for a substitution function to equate to zero only the first $\frac{1}{2}(p-1)$ of the expressions given by Hermite.

§ 2. Application to particular cases.

In the case of five letters we may take $a_1 z^3 + a_2 z^2 + a_3 z$ for the general form of substitution function, so that the condition $s_1 \equiv 0$ holds good for modulus 5.

By the above theorem the only other necessary condition is that $s_2 \equiv 0$, that is

$$2a_1 a_3 + a_2^2 \equiv 0.$$

The solution of this congruence includes three cases:

$$(1)\ \begin{cases} a_1 \equiv 0 \\ a_2 \equiv 0 \end{cases} \qquad (2)\ \begin{cases} a_3 \equiv 0 \\ a_2 \equiv 0 \end{cases} \qquad (3)\ \left\{ a_3 \equiv \frac{2a_2^3}{a_1}, \right.$$

where in the third case we suppose none of the coefficients to be zero-congruent.

The first case gives us $a_3 z$; the second $a_1 z^5$; the third $a_1^3 (a_1 z + 2a_2)^5 + 2a_1^2 a_2^3$, which is included in the generalized form $\alpha\phi(z+\beta)+\gamma$, where $\phi z \equiv z^5$.

We see then that $s_1 \equiv 0$, $s_2 \equiv 0$ gives us all possible forms of substitution functions of five letters, as given in Serret § 485.

In the case of seven letters it is better to refer to the investigation of the subject in Serret's *Alg.*, § 486.

In the case taken first there, it will be seen that only the second and third powers of $z^4 + az^2 + bz$ are treated of, and when the corresponding function $z^4 \pm 3z$ is obtained, it is shewn that all Hermite's conditions hold good.

A similar process is gone through with regard to the form $z^5 + az^3 + bz^2 + cz$, for which the conditions corresponding to $s_2 \equiv 0$, $s_3 \equiv 0$, and $s_4 \equiv 0$ are written down. It is proved, however, that the values of a, b, c obtained from $s_2 \equiv 0$, $s_3 \equiv 0$ are identically satisfied by $s_4 \equiv 0$ in the general case; while $s_5 \equiv 0$ is proved to hold good in each separate case.

Hence, the above theorem is verified in the cases when the modulus is 5 or 7.

A further question arises with regard to Hermite's conditions, as to whether other relations exist among them so as to further reduce the number of independent conditions. In other words, given a congruence whose roots are all real for a prime modulus p, how many conditions of the form $s_r \equiv 0$ are just sufficient to ensure that $s_r \equiv 0$ for all values of r except when r is a multiple of $p-1$?

The problem before us admits of many difficulties, but in the case when $p = 11$, it can be proved by a direct method that unless $s_1 \equiv 0 \equiv s_2 \equiv s_3 \equiv s_4 \equiv s_5$, there exist congruences with real roots other than $z^{11} - z \equiv 0$.

For instance, the conditions $s_1 \equiv 0 \equiv s_2 \equiv s_3 \equiv s_4$ are not sufficient to make s_r generally $\equiv 0$, for the congruence whose roots are zero, and each quadratic residue taken twice, satisfies the conditions, viz., $z(z^5-1)^2 \equiv 0$, and in this case $s_5 \equiv 10$.

Similarly the congruence whose roots are 0, 1, 1, 1, 1, 5, 6, 6, 6, 7, 10 satisfies the four conditions $s_1 \equiv 0 \equiv s_2 \equiv s_4 \equiv s_5$; that whose roots are 0, 1, 2, 2, 2, 3, −3, −2, −2, −2, −1

satisfies the four conditions $s_1 \equiv 0 \equiv s_2 \equiv s_3 \equiv s_5$, and the conditions $s_1 \equiv 0 \equiv s_3 \equiv s_4 \equiv s_5$ hold good for the quantic whose roots are the cubes of the last. Thus we see that as far as the simplest conditions are concerned, four of the conditions $s_1 \equiv 0 \equiv s_2 \equiv s_3 \equiv s_4 \equiv s_5$ are not sufficient to make all the roots different.

On the other hand, we may choose five of Hermite's conditions which shall not necessitate the other four, as in the case where the congruence only contains odd powers of z, so that $s_1 \equiv 0 \equiv s_3 \equiv s_5 \equiv s_7 \equiv s_9$. Since, however, it is evident that the lowest powers give the simplest relations, it seems scarcely worth while to investigate whether any four more complicated ones such as $s_1 \equiv 0 \equiv s_3 \equiv s_7 \equiv s_8$ are sufficient to include all the other conditions.

EXPRESSION FOR THE SUM OF THE CUBES OF THE DIVISORS OF A NUMBER IN TERMS OF PARTITIONS OF INFERIOR NUMBERS.

By *J. W. L. Glaisher.*

It was shown by Euler that, if $P(n)$ denote the number of partitions of n into the numbers 1, 2, 3, ..., repetitions not excluded, and if $P(0)$ have the value unity, then

$$P(n) - P(n-1) - P(n-2) + P(n-5) + P(n-7) - \&c. = 0,$$

where 1, 2, 5, 7, ..., are the pentagonal numbers $\frac{1}{2}(3r^2 \pm r)$ and the signs of the term are positive or negative according as r is even or uneven.*

It is easy to show that

$$P(n-1) + 2P(n-2) - 5P(n-5) - 7P(n-7) + \&c. = \sigma(n),$$

where $\sigma(n)$ denotes the sum of the divisors of n.

I have also found that

$$P(n-1) + 2^3 P(n-2) - 5^3 P(n-5) - 7^3 P(n-7) + \&c. = -\tfrac{1}{12}\{5\sigma_3(n) - (18n-1)\,\sigma(n)\},$$

where $\sigma_3(n)$ denotes the sum of the cubes of the divisors of n.

---

* Euler, *Commentationes Arithmeticæ Collectæ*, Vol. i., p. 91. See also *Proc. Lond. Math. Soc.*, Vol. xxi., p. 202.