# NOTE ON A SYSTEM OF LINEAR CONGRUENCES

*By* J. CULLEN.

[Received April 7th, 1904.—Read April 14th, 1904.]

GAUSS (*Werke*, Vol. II., pp. 507–509) has given a table from which the linear forms of $H$ in the equation

$$N = lH^2+mG^2$$

are easily obtained. In a previous communication* the writer has given a general process for solving any linear system. When, however, $H$ is ambiguous in sign the work in applying this process can be considerably reduced. The object of the present note is to explain this briefly.

[The results in the present paper are numbered with accented figures, thus: 1′, 2′, &c. References with unaccented figures (as 1, 2, &c.) relate to the numbered results in the original paper.]

1. In the system § 2 of the original paper it is clear that the solution arising out of the selection of one residue in each row is quite independent of the value of any of the other residues.

Thus, for instance, in

$$H \equiv a_l \,(\text{mod } P) \equiv \beta_s \,(\text{mod } Q) \equiv \rho'_t \,(\text{mod } p'),$$

$H$ in no way depends on the other residues.

Hence we may introduce

$$a_0 \equiv 0 \ (\text{mod } P), \qquad \beta_0 \equiv 0 \ (\text{mod } Q),$$

provided (i.) the redundant cases are subsequently excluded, (ii.) the actual cases in which 0 occurs are retained.

Since the symbol $\kappa$ in the set row of each strip refers to the case $a_\kappa$, and $\varpi$ in the arrangement row of each strip to the case $\beta_\varpi$, the case $a_0$ is excluded or retained, according as the symbol 0 is not written or is written in the set rows. In like manner, $\beta_0$ is excluded by not using the arrangement in which 0 occurs in the arrangement rows, though 0 is always written in the initial division of the arrangement row of each strip.

2. The effect of introducing 0 in each row of the given system, where it is wanting, is that

(i.) The preliminary work is much simplified, for $a_0 \equiv 0$, $\beta_0 \equiv 0$ now take the place of $a_1$, $\beta_1$ in the determination of the $\lambda$'s and the $r$'s in p. 325;

* *Proc. London Math. Soc.*, Vol. XXXIV., pp. 323–334.

(ii.) The equation (10) becomes simply

$$H = xPQ + r_{\varpi,0} + r_{0,\kappa}, \qquad \text{since} \qquad r_{0,0} = 0\,;$$

(iii.) The headings of the columns of the elements table, p. 333, become $r_{0,0}$, $r_{0,1}$, $r_{0,2}$, ..., $r_{1,0}$, $r_{2,0}$, $r_{3,0}$, ..., with 0 throughout the first column; and hence, because 0 is written in the initial division of the arrangement rows, this division is now always placed under the 0 in each line of the base sheet when finding the arrangement numbers, instead of different numbers for different strips, as given by Rule III.

In short, we proceed exactly as in the paper, with this difference: that the subscript 0 is substituted for 1 in the preliminary work and elements table, and the question of the retention or rejection of $\alpha_0$, $\beta_0$ (it rarely happens that these are to be retained) is to be considered.

3. The remarks of the foregoing paragraphs apply to any linear system whatever. In what follows we consider a linear system in which there exists an ambiguity in sign for every residue, as is always the case in $H$ where

$$aH^2 \pm bG^2 = N.$$

The same ambiguity arises also in the residues obtained by combining different moduli. In fact, we always have

$$a(\pm H)^2 \pm b(\pm G)^2 = N.$$

4. In a system of the given type,

$$\begin{aligned} H &\equiv \pm\alpha_1,\ \ \pm\alpha_2,\ \ \pm\ldots,\ \ \pm\alpha_m \pmod{P} & (1') \\ &\equiv \pm\beta_1,\ \ \pm\beta_2,\ \ \pm\ldots,\ \ \pm\beta_n \pmod{Q} & (2') \\ &\equiv \pm\rho_1',\ \ \pm\rho_2',\ \ \pm\ldots,\ \ \pm\rho_f' \pmod{p'} & \\ &\ldots\quad \ldots\quad \ldots\quad \ldots\quad \ldots & \\ &\equiv \pm\rho_1^{(\sigma)},\ \pm\rho_2^{(\sigma)},\ \pm\ldots,\ \pm\rho_s^{(\sigma)} \pmod{p^{(\sigma)}}, & \end{aligned}$$

we are merely concerned with the congruences (1′) and (2′). As to the others, we need only supply 0 where it is absent, and proceed as in the original paper (pp. 323–334), dotting only the given 0's.

If we make all the residues in (1′) positive, and arrange them according to the order of magnitude, we have, on taking $\alpha_1$, the smallest, and $\alpha_{2m}$, the greatest,

$$H \equiv \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_m,\ \alpha_{m+1},\ \ldots,\ \alpha_{2m} \pmod{P}.$$

Now, call $\alpha_\varpi$, $\alpha_{\varpi'}$ complementary residues where

$$\alpha_\varpi + \alpha_{\varpi'} = P. \qquad (3')$$

We then have also

$$\varpi + \varpi' = 1 + 2m. \qquad (4')$$

5. It is now easy to show that $r_{\varpi,0}$, $r_{\varpi',0}$ are complementary with respect to the modulus $PQ$ if $\varpi+\varpi' = 2m+1$. For, by (3), (5), (7), p. 324, we have

$$r_{\varpi,0} = P\lambda_{\varpi,0}+a_{\varpi} \equiv uPa_{\varpi}+a_{\varpi} \pmod{PQ} \equiv Qva_{\varpi} \pmod{PQ}.$$

Also $$r_{\varpi',0} \equiv Qva_{\varpi'} \pmod{PQ}.$$

Therefore, by (3′), $r_{\varpi,0}+r_{\varpi',0} \equiv 0$; so that, taking $r_{\varpi,0}$, $r_{\varpi',0}$ as least positive residues, then

$$r_{\varpi,0}+r_{\varpi',0} = PQ. \tag{5′}$$

In a precisely similar manner we find that, if $\kappa+\kappa' = 2n+1$, then

$$r_{0,\kappa}+r_{0,\kappa'} = PQ. \tag{6′}$$

6. From (5′) and (6′) it follows that, having found $r_{\varpi,0}$ and $r_{0,\kappa}$, it is not necessary to apply the congruences, p. 325, to find $r_{\varpi',0}$ and $r_{0,\kappa'}$, $\varpi'$ ranging from $m+1$ to $2m$, and $\kappa'$ from $n+1$ to $2n$. A similar remark applies to $\theta_{\varpi',0}$ and $\theta_{0,\kappa'}$ in the elements table for every row (1 to $\sigma$), since we have for any prime $p^{(\tau)}$, by (5′) and (6′),

$$\theta^{(\tau)}_{\varpi',0} \equiv t^{(\tau)}-\theta^{(\tau)}_{\varpi,0} \pmod{p^{(\tau)}}, \qquad \theta^{(\tau)}_{0,\kappa'} \equiv t^{(\tau)}-\theta^{(\tau)}_{0,\kappa} \pmod{p^{(\tau)}}.$$

It is not even necessary to complete the elements table in this manner; for all we really require are the residues ($\theta$) and ($t$) for the columns under $r_{0,0}, r_{0,1}, \ldots, r_{0,n}$; $r_{1,0}, r_{2,0}, \ldots, r_{m,0}, PQ$. This is easily seen, as follows.

7. To find the arrangement numbers for the strip $p'$, say, write 0 in the initial division and place this division under the 0 of the $p'$ line of the base sheet, writing $1, 2, \ldots, m$ under the $t'$'s that equal $\theta'_{1,0}, \theta'_{2,0}, \ldots, \theta'_{m,0}$, and $m+1, m+2, \ldots, 2m$ under the $t'$'s that equal $(t'-\theta'_{m,0}), (t'-\theta'_{m-1,0}), \ldots, (t'-\theta'_{1,0})$ respectively. This is nothing more than writing the corresponding subscripts of the complementary residues. [Cf. (5′).]

It will be noticed that $\varpi$ and $\varpi'$ are equally distant from the centre of the strip; in fact, since $\theta'_{\varpi,0} \equiv xt'$ and $\theta'_{\varpi',0} \equiv x't'$, we have, by (5′),

$$xt+x't' \equiv t' \pmod{p'} \qquad \text{or} \qquad x+x' \equiv 1 \pmod{p'};$$

so that $x+x' = 1+p'$ if $x > 0 < p'$, $x' > 0 < p'$, $x$ and $x'$ being the numbers in the base line over $\theta'_{\varpi,0}$, $\theta'_{\varpi',0}$.

[*Ex. gr.*—In the base sheet facing p. 334, for $p = 17$ say, and $\theta_{\varpi,0} \equiv 15$, then $\theta_{\varpi',0} \equiv 11-15 \equiv 13$, the numbers in the base line over 15 and 13 are $x = 6$, $x' = 12$, and $6+12 = 1+17$. Similarly for other cases.]

This serves as a useful check in writing down the arrangement numbers.

8. Having seen that the number of columns of the elements table giving the arrangement numbers may consist simply of $m$ columns,

instead of $2m$, we can now show by (6′) that a similar result holds for the columns giving the set numbers, viz., that we need only $n$ instead of $2n$ columns* (since $r_{0,0} = 0$).

For suppose that a solution is

$$H = xPQ + r_{\varpi', 0} + r_{0, \kappa'};$$

we can, by searching to the left of the 0 of the base line, make $x$ negative, and hence, if $x = -y$ $(y > 0)$, then

$$H = -(yPQ - r_{\varpi', 0} - r_{0, \kappa'}) = -\{(y-2)PQ + r_{\varpi, 0} + r_{0, \kappa}\};$$

and, as $H$ is itself ambiguous in sign, there must also be the positive solution

$$H = (y-2)PQ + r_{\varpi, 0} + r_{0, \kappa}.$$

In other words, since $x$ and $y$ are numerically equal, we have the result that, if $\kappa'$ appears throughout the strips in the arrangement $\varpi'$ under $x$ on the left of the 0 of the base line (thus: ..., 5, 4, 3, 2, 1, 0, 1, 2, 3, 4, 5, ...), then $\kappa$ appears throughout in the arrangement $\varpi$ under $x-2$ on the right of the base line's 0, where

$$\varpi + \varpi' = 2m+1, \qquad \kappa + \kappa' = 2n+1.$$

As these solutions are numerically equal (in fact, complementary with respect to the modulus that is the product of all the moduli), we may obviously exclude one, which is done at once by excluding the set numbers $\kappa'$ that range from $n+1$ to $2n$.

9. In brief, therefore, in the linear system arising from the equation

$$N = lH^2 + mG^2$$

we may neglect all ambiguity in sign in the $\alpha$'s and $\beta$'s (so that no two complements ever occur in the system), and proceed as in the original paper, with the addition of reading to the left, and, if $\kappa$ appears throughout the arrangement $\varpi$ under $x$ on the left, then the solution is

$$H = -xPQ + r_{\varpi, 0} + r_{0, \kappa}.$$

10. The case $N = H^2 - G^2$, where $N$ is a factor of $a^z \pm 1$, requires special treatment, since it is known that every factor of $a^z \pm 1$ is of the form $Rz+1$. It is further known that, generally, $H = z^2L + M$: hence we have a row

$$H = a_1, a_2, a_3, \ldots, a_m \pmod{z^2P},$$

in which none of the $a$'s are complementary. It is, however, easy to see that all that is required is to proceed in the manner explained above in searching to the right of the 0 of the base line, but in searching to the left we take the complementary arrangements and deal only with these.

* A considerable saving in the labour of drawing up the strips. It also extends the scope of the process.