

A PROPERTY OF NUMBERS.

BY F. C. AULUCK AND S. CHOWLA.

(Government College, Lahore.)

Received May 29, 1937.

1. **THEOREM.** *Let p be a prime. If the numbers $r, r + s, r + 2s, \dots, r + (m - 1)s$ are congruent* (mod p) to the numbers $0, 1, 2, \dots, (m - 1)$ [not necessarily in this order], then if $m < p - 1$, we must have either $r = 0, s = 1$ or $r = m - 1, s = -1$.*

Remarks. (i) If $m = p$ the numbers $r + ts$ ($0 \leq t \leq m - 1$) are congruent to the numbers $0, 1, 2, \dots, m - 1$ for any values of r and s provided s is prime to p .

(ii) If $m = p - 1$ the theorem is false for we can take any $s \not\equiv \pm 1$ and then choose $r \equiv s - 1$.

Proof. If the set

(1) $r, r + s, \dots, r + (m - 1)s \equiv 0, 1, 2, \dots, (m - 1)$ in some order, then by addition from (1),

$$(2) \quad mr + \frac{sm(m-1)}{2} \equiv \frac{m(m-1)}{2}$$

since $m < p$, this gives

$$(3) \quad r \equiv -\frac{(s-1)(m-1)}{2}.$$

Again, from (1),

$$\sum_{t=0}^{m-1} (r + ts)^2 \equiv \sum_{t=0}^{m-1} t^2$$

Using (3), this becomes

$$\begin{aligned} \frac{m(m-1)^2(s-1)^2}{4} - \frac{s(s-1)m(m-1)^2}{2} \\ + (s^2 - 1) \frac{m(m-1)(2m-1)}{6} \equiv 0 \end{aligned}$$

or

$$\frac{m(m-1)(s-1)}{12} \left\{ 3(m-1)(s-1) - 6s(m-1) + 2(s+1)(2m-1) \right\} \equiv 0$$

or

$$\frac{m(m-1)(s-1)}{12} \left\{ (m+1)(s+1) \right\} \equiv 0$$

since $m < p - 1$ this implies $s \equiv \pm 1$. Our result follows immediately.

2. We have also obtained a "pictorial" proof of the above theorem, by arranging the numbers on the unit circle, the number r being represented by $e^{2\pi i r/p}$.

* All congruences are to the modulus p .