On the solution of some special linear congruences.

By G. SZÁSZ in Szeged.

In this paper letters A, B, M, a, b, m, n denote positive integers; $\left(\frac{B}{A}\right)_M$ means the least positive integer solution of the congruence

$$(1) \qquad Ax \equiv B \pmod{M}.$$

This congruence may always be reduced to the form

$$ax \equiv b \pmod{m},$$

where $0 < b < a$, $(a, b) = 1$. If (1) has any solution, then $(a, b) = 1$ implies $(a, m) = 1$. For such congruences we shall prove the following

Theorem 1. *If* $0 < b < a$, $(a, b) = 1$, $m \equiv n \pmod{a}$, *then*

$$(2a) \qquad \frac{a\left(\frac{b}{a}\right)_m - b}{m} = \frac{a\left(\frac{b}{a}\right)_n - b}{n},$$

i. e., if b is fixed,

$$(2b) \qquad \bar{m} = \frac{a\left(\frac{b}{a}\right)_m - b}{m}$$

is an invariant of the residue class m $\pmod{a}$.

Proof. (2b) implies

$$(2c) \qquad m\bar{m} = a\left(\frac{b}{a}\right)_m - b;$$

hence

$$(3) \qquad m\bar{m} \equiv -b \pmod{a},$$

where $(a, m) = 1$; thus $\bar{m}$ belongs to a determined residue class mod a. It is obvious that $\bar{m}$ is a positive integer $< a$; consequently, $\bar{m}$ is the least positive solution of (3).

From (3) we infer also that $(a, \bar{m}) \mid b$. As $(a, b) = 1$, we have $(a, \bar{m}) = 1$: $\bar{m}$ belongs to the reduced system of residues mod a.

Corollary. A simple rearrangement of (2a) gives

$$m\left(\frac{b}{a}\right)_n - n\left(\frac{b}{a}\right)_m = (m-n)\frac{b}{a}.$$

This formula gives a method to determine the least positive solution of the congruences by reduction to other congruences with smaller modules. (An other method by use of continued fractions is well-known.)

Consider now the $\overline{m}$ defined by (2b). We prove

Theorem 2. *If* $0 < b < a$, $(a\ b) = 1$,

$$\overline{m} = \frac{a\left(\frac{b}{a}\right)_m - b}{m}, \tag{4}$$

then the mapping $m \to \overline{m}$ *for* $m < a$ *is a permutation* P_b *of the reduced system of residues mod* a, *for which* $P_b^2 = I$.[1]) *Permutat ons* P_b *generated by different* b*'s are different.*

Proof From the conditions of theorem 2 and from the proof of theorem 1 it follows that

$$0 < m,\ \overline{m} < a$$

and

$$(a\ m) = (a, \overline{m}) = 1$$

If $m < a$, we get from (3) also that $m \to \overline{m}$ is an one-to-one mapping (i. e. a permutation) of the reduced system of residues mod a.

Clearly, $P_b = P_{b'}$ if and only if $b = b'$ (this follows from (3), because $b, b' < a$). From (2c) we get first

$$a\left(\frac{b}{a}\right)_m \equiv b \pmod{\overline{m}};$$

next, as $m, \overline{m} < a$,

$$\left(\frac{b}{a}\right)_m < \overline{m}.$$

These results mean that $\left(\frac{b}{a}\right)_m = \left(\frac{b}{a}\right)_{\overline{m}}$, i. e. if

$$P_b(m) = \overline{m}$$

then we have also

$$P_b(\overline{m}) = m.$$

But this is equivalent to $P_b^2 = I$.

Remark. It is possible that the set of all P_b forms a group. If it is so, then we have $P_{b_0} = I$ for some b_0; choosing $m = 1$ we obtain $\overline{m} = a - b_0$. Consequently we have $b_0 = a - 1$.

On the other hand, $P_{b_0} = I$ means that $\overline{m} = m$ and it follows from (3) that

$$m^2 \equiv -b_0 \pmod{a};$$

[1]) I is the identical permutation.

hence

(5) $$m^2 \equiv 1 \pmod a$$

for all m subjected only to the condition $(a, m) = 1$. The number of all such m is $\varphi(a)$, where $\varphi(a)$ denotes EULER's φ-function. If $\varkappa(a)$ denotes the number of solutions of (5), then we must have $\varkappa(a) = \varphi(a)$. It is easy to verify that this condition is satisfied only if a is a divisor of 24.

Conversely, it turns out by direct computation that for each such value of a, the set of permutations P_b forms a group.

(Received May 19, 1950.)