An elementary semigroup theorem and a congruence relation of Rédei.

By ŠTEFAN SCHWARZ in Bratislava (ČSR).

RÉDEI proved the following theorem: Let $m > 1$ be an integer, $\varphi(m)$ the Euler function. Then every integer x satisfies the relation

$$x^m \equiv x^{m-\varphi(m)} \pmod{m}. \tag{1}$$

If $m = p$ is a prime, (1) has the form $x^p \equiv x \pmod{p}$; hence (1) is a generalization of the theorem of FERMAT.

An elementary proof of (1) is given in [1], p. 132.

The purpose of this note is to show that (1) is a special case of a general theorem concerning finite semigroups.

The proof of (1) based on the theory of semigroups seems to be of some interest, since in spite of advances of the theory of semigroups in the last years non-trivial applications to the elementary theory of numbers are rather sporadic.

For convenience of the reader we recall in section 1 some elementary facts concerning finite semigroups. The general theorem mentioned above will be given in section 2. In section 3 we give the application to the proof of RÉDEI's theorem.

1.

Let S be a finite semigroup and $a \in S$. The sequence

$$a, a^2, a^3, \ldots \tag{2}$$

contains a finite number of different elements. Denote by $\varrho(a)$ and $\sigma(a)$, the smallest integers with $a^{\varrho(a)} = a^{\sigma(a)}$, $\varrho(a) < \sigma(a)$. It is well known that (2) contains then exactly $\sigma(a) - 1$ different elements. These are

$$a, a^2, \ldots, a^{\varrho(a)-1}, a^{\varrho(a)}, \ldots, a^{\sigma(a)-1}. \tag{3}$$

The set $\{a^{\varrho(a)}, \ldots, a^{\sigma(a)-1}\} = \mathfrak{g}_a$ is a group. The number $l_a = \sigma(a) - \varrho(a)$ will

be called the period of a. For every $\lambda \geqq \varrho(a)$ the element a^λ is contained in $\mathfrak{g}_a$ and $a^\lambda = a^{\lambda+\tau l_a}$ holds for all integers $\tau > 0$.

The set (3) contains exactly one idempotent e, namely, the unit of $\mathfrak{g}_a$. We shall say that a belongs to the idempotent e.

Denote by P_e the set of all elements $\in S$ belonging to a fixed idempotent e. Then S can be written as the class sum of disjoint subsets $S = \sum P_e$, where e runs through all idempotents $\in S$.

To every e there exists a unique maximal group G_e having e as unit element. Cleary $G_e \subseteqq P_e$. The group G_e contains exactly all $x \in P_e$ for which $xe = ex = x$ holds. It is therefore $e \cdot P_e = P_e \cdot e = G_e$.

If S contains a unit element e_1 (more generally a one-sided unit element e_1), then $P_{e_1} \cdot e_1 = P_{e_1}$, hence $P_{e_1} = G_{e_1}$, i. e. the set of elements $\in S$ belonging to the unit element (one-sided unit element) forms a group.

2.

Let now be S a finite semigroup of order $m > 1$ with a two-sided unit e_1 and the corresponding maximal group G_1.

We shall show: If S is not a group, then $S - G_1$ is a semigroup. This assertion is known. Nevertheless we give a short proof. Let be $b \in S - G_1$. We prove first $Sb \cap G_1 = \mathfrak{0}$. The proof follows indirectly. Suppose $a \in Sb \cap G_1$. Then there is a b^* with $a = b^* b$. Find an $a^* \in G_1$ with $a^* a = e_1$. Then $a^* b^* b = e_1$. Denote $c = a^* b^*$; then $cb = e_1$. Since $b \in S - G_1$, b belongs to an idempotent $e' \neq e_1$, i. e. there exists an integer $\varrho > 0$ such that $b^\varrho = e' \neq e_1$. The relation $cb = e_1$ implies $c(cb) \cdot b = ce_1 b = cb = e_1, c^2 b^2 = e_1$. Repeating this argument we have $c^\varrho b^\varrho = e_1$, i. e. $c^\varrho e' = e_1$. Hence $e_1 = c^\varrho e' = c^\varrho (e' e') = (c^\varrho e') e' = e_1 e' = e'$, which is a contradiction. For every $b \in S - G_1$ we have $Sb \subset S - G_1$, hence $S(S - G_1) \subset S - G_1$ and the more $(S - G_1)^2 \subset S - G_1$. This shows that $S - G_1$ is a semigroup.

Denote the order of G_1 by l.

Suppose first $x \in G_1$. Then $x^l = e_1$. If $m > l$ we have $x^{m-l} \in G_1$. Hence $x^{m-l} \cdot e_1 = x^{m-l}$. On the other side we have $x^{m-l} \cdot e_1 = x^{m-l} \cdot x^l = x^m$. Therefore

$$x^m = x^{m-l}.$$

(This result holds also for $m = l$, if x^0 denotes the unit element of G_1.)

Suppose for the rest that $m > l$ and $x \in S - G_1$. The semigroup $S - G_1$ is of order $m - l$. Hence the set

(4) $$x, x^2, \ldots, x^{m-l}$$

contains (a unique) idempotent e. There exists therefore an integer k,

$1 \leqq k \leqq m-l$, with $x^k = e$. The intersection of the maximal group G_e with the set (4) is the group $\mathfrak{g}_x$. Since $k \leqq m-l$, we have $x^{m-l} \in \mathfrak{g}_x$. If l_x is the period of x there holds

$$x^{m-l} = x^{m-l+\tau l_x}$$

for every non-negative integer τ.

Suppose now that l_x is a divisor of l. Then there is a $\tau \geqq 1$ such that $-l+\tau l_x = 0$. Hence $x^{m-l} = x^m$.

Thus we have proved:

Theorem. *Let S be a finite semigroup of order m having a unit element e_1. Denote by l the order of the maximal group belonging to e_1. If the period of every $x \in S$ is a divisor of l, then*

$$x^m = x^{m-l}$$

holds for every $x \in S$.

Remark. This theorem can be generalized as follows. Suppose that S has exactly s right units. It is known (see [2] and [3]) that the maximal groups $G_1^{(1)}, \ldots, G_1^{(s)}$ belonging to these idempotents are isomorphic and the set $S-(G_1^{(1)}+\cdots+G_1^{(s)})$ is a semigroup. (In fact it is an ideal of S.) An analogous argument as above shows the validity of the following theorem:

Let S has exactly s right units and let l be the (common) order of the maximal groups belonging to each of them. If the period of all $x \in S$ divides ls, then every $x \in S$ satisfies the relation $x^m = x^{m-sl}$.

3.

We shall show now that the theorem of RÉDEI is a special case of our theorem.

Let $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\alpha_1 > 0, \ldots, \alpha_r > 0$ be the factorization of $m > 0$ into different primes. Let S_m be the semigroup of residue classes (mod m). The class containing the number x will be denoted by $[x]$.

The maximal group belonging to $[1]$ is the set of all $[a] \in S_m$ with $(a, m) = 1$. Its order is $\varphi(m)$. To prove (1) it is sufficient to show that *the period of each $[x] \in S_m$ divides $\varphi(m)$.*

Let be $[x] \in S_m$. By rearranging suitably the primes we can suppose that $[x]$ is of the form

$$[x] = [p_1^{k_1} \cdots p_s^{k_s} a],\ 0 \leqq s \leqq r,\ k_1 \geqq 1, \ldots, k_s \geqq 1,$$

with $(a, m) = 1$. (The case $s = 0$ means $[x] = [a]$ with $(a, m) = 1$. In this case

$[x]$ is an element of a group of order $\varphi(m)$ and our assertion is trivially true.) The relation $[x]^\varrho = [x]^\sigma$ with $1 \leqq \varrho \leqq \sigma$ implies

$$(p_1^{k_1} \cdots p_s^{k_s} a)^\varrho = (p_1^{k_1} \cdots p_s^{k_s} a)^\sigma \pmod m,$$

i. e.

$$(5) \qquad (p_1^{k_1} \cdots p_s^{k_s} a)^\varrho \{(p_1^{k_1} \cdots p_s^{k_s} a)^{\sigma-\varrho} - 1\} \equiv 0 \pmod{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}.$$

a) If $s = r$, then there exists such a $\varrho > 0$ that

$$(p_1^{k_1} \cdots p_r^{k_r} a)^\varrho \equiv 0 \pmod{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}.$$

Let ϱ_1 be the smallest such ϱ. The relation $[x]^{\varrho_1} = [0]$ implies $[x]^{\varrho_1+1} = [x]^{\varrho_1}$. All elements of the form considered have the period equal to 1 and our assertion is true.

b) Suppose $0 < s < r$. To satisfy (5) we must first choose ϱ such that

$$(p_1^{k_1} \cdots p_s^{k_s})^\varrho \equiv 0 \pmod{p_1^{\alpha_1} \cdots p_s^{\alpha_s}}.$$

Let ϱ_1 be the smallest such ϱ. The congruence (5) will then be satisfied if and only if $\sigma > \varrho_1$ is such that

$$(6) \qquad (p_1^{k_1} \cdots p_s^{k_s} a)^{\sigma-\varrho_1} - 1 \equiv 0 \pmod{p_{s+1}^{\alpha_{s+1}} \cdots p_r^{\alpha_r}}.$$

But $(p_1^{k_1} \cdots p_s^{k_s} a, p_{s+1}^{\alpha_{s+1}} \cdots p_r^{\alpha_r}) = 1$. Denote by σ_1 the smallest σ satisfying (6). Then $\sigma_1 - \varrho_1$ is either $\varphi(p_{s+1}^{\alpha_{s+1}} \cdots p_r^{\alpha_r})$ or a divisor of this number. Hence $\sigma_1 - \varrho_1$ divides $\varphi(m)$, i. e. the period of every element $[x] \in S_m$ divides $\varphi(m)$, q. e. d.

References.

[1] W. Sierpiński, *Arytmetyka teoreticzna* (Warszawa, 1955).

[2] Št. Schwarz, Topological semigroups with one-sided units, *Czechoslovak Math. Journal*, **5 (80)** (1955), 153-163.

[3] W. M. Faucett—R. J. Koch—K. Numakura, Complements of maximal ideals in compact semigroups, *Duke Math. Journal*, **22** (1955), 655-662.

(Received September 23, 1957.)