Collect. Math. **46**, 1–2 (1995), 183–193

Universal formulae of Euler-Fermat type for subsets of Z_m

Štefan Schwarz

Mathematical Institute, Slovak Academy of Sciences
Štefánikova 49, SK 814-73 Bratislava, SLOVAKIA

Dedicated to the memory of Paul Dubreil

Abstract

In several papers Paul Dubreil has studied the multiplicative semigroup of several types of rings and conditions for semigroups which can serve as an underlying semigroup of a ring. In this paper we shall deal with the multiplicative semigroup of Z_m, which will be denoted by $S(m)$, and we shall treat a rather unconventional problem concerning the powers of a subset of $S(m)$.

In several papers Paul Dubreil has studied the multiplicative semigroup of several types of rings and conditions for semigroups which can serve as an underlying semigroup of a ring. In particular he studied rings which have analogous additive properties as Z_m. (See, e.g., [1], [2]).

In this paper we shall deal with the multiplicative semigroup of Z_m, which will be denoted by $S(m)$, and we shall treat a rather unconventional problem concerning the powers of a subset of $S(m)$.

We first formulate the problem in a more general setting. Let S be a finite semigroup and P a non-empty subset of S, $|S| = n$. Consider the sequence of powers $\{P, P^2, P^3, \ldots\}$. Clearly this sequence contains only a finite number of different sets. Let $k = k(P)$ be the least integer for which $P^k = P^t$ for some $t > k$. Let further $d = d(P) \geq 1$ be the smallest integer for which $P^k = P^{k+d}$. Then the sequence of powers has the following form

$$P, P^2, \ldots, P^{k-1} | \, P^k, \ldots, P^{k+d-1} | \, P^k, \ldots .$$

It is well-known that the sets in the "periodic part" $\{P^k, \dots, P^{k+d-1}\}$ considered as elements of the power semigroup of S (with an obvious multiplication) form a cyclic group of order d. More precisely: Let $\beta \geq 1$ be the uniquely determined integer such that $k \leq \beta d \leq k+d-1$. Denote $r = \beta d$, $r = r(P)$, then P^r is the identity element of the group just considered. Also P^r considered as a subset of S is a subsemigroup of S satisfying $P^r = P^{r+d} = P^{2r}$.

The main problem is to find estimations for $k(P)$ and $d(P)$ in terms of $n = |S|$.

We now explain the title of the paper.

Recall the following known fact. Let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ be the canonical factorization of $m (p_i = \text{primes}, \alpha_i \geq 1)$. Denote $\nu(m) = \{\max \alpha_i \,|\, i = 1, \dots, s\}$. Then for any $x \in S(m)$ we have $x^{\nu(m)} = x^{\nu(m)+\lambda(m)}$, where $\lambda(m)$ is the *Carmichael* function. (See, e.g., [4].) This is a universal formula in the sense that it holds for all $x \in S(m)$, otherwise expressed the exponents depend only on m. [This formula is the strongest possible generalization of the classical Euler–Fermat formula $x = x^{1+\varphi(m)}$ which holds for $(x, m) = 1$.]

Let now be P a subset of $S(m)$. Then the integers k and d satisfying $P^k = P^{k+d}$ with smallest k and d depend on P. If we are able to find integers k^* and d^* such that $P^{k^*} = P^{k^*+d^*}$ holds for all subsets $P \subset S(m)$, we shall say that this is a universal formula of the Euler–Fermat type. Clearly, we shall try to find k^*, d^* as small as possible.

I. Some general statements

In this section we give some results, which hold for any finite semigroup S.

The numbers $k(P)$, $d(P)$ and $r(P)$ have the meaning defined in the introduction.

Suppose $|S| = n$ and $P \subset S$. The subsemigroup of S generated by P is the semigroup $\overline{P} = P \cup P^2 \cup \dots \cup P^{n_o}$, where clearly $n_0 \leq n - |P| + 1$. Also the set $\hat{P} = P^k \cup P^{k+1} \cup \dots \cup P^{k+d-1}$ is a subsemigroup of S, and we have $P^r \subset \hat{P} \subset \overline{P}$. Denote $|\overline{P}| = n_1$. We have $n_0 \leq n_1 \leq n$.

Note also that the system of sets $\{P^k, \dots, P^{k+d-1}\}$ is (up to the ordering) identical with the system of sets $\{P^r, P^{r+1}, \dots, P^{r+d-1}\}$.

For formal calculations it is rather convenient to denote $Q = P^{r+1}$. Then $Q^2 = P^{2(r+1)} = P^{r+2}, \dots, Q^{d-1} = (P^{r+1})^{d-1} = P^{r+d-1}$ and $Q^d = P^r$. [Note that $Q^\alpha \cdot P^\beta = Q^{\alpha+\beta}$]. Hence the system of sets $\{Q, Q^2, \dots, Q^d\}$ is again (up to the ordering) identical with the system $\{P^k, P^{k+1}, \dots, P^{k+d-1}\}$ and $\hat{P} = Q \cup Q^2 \cup \dots \cup Q^d$. In the following we shall often denote $P^r = Q^d = Q_0$.

Our original sequence has now the form

$$P, P^2, \dots, P^{k-1} \big| P^k = Q^k,\ P^{k+1} = Q^{k+1}, \dots, P^{k+d-1} = Q^{k+d-1} \big| \dots$$

(Here, of course, $Q^{\alpha+d} = Q^{\alpha}$.)

The sets $Q, Q^2, \dots, Q^d$ are – in general – not disjoint, but the following holds.

Lemma 1

If $d = d(P) > 1$, then none of the sets $Q, Q^2, \dots, Q^d$ is a proper subset of any of the others.

Proof. Suppose for an indirect proof that $Q^u \subset Q^v$, $1 \le u < v \le d$. Multiplying by Q^{d-u} we have $Q^d \subset Q^{d+(v-u)}$, hence $Q_0 \subset Q^{v-u}$. Denote $v - u = \gamma < d$.

$$Q_0 \subset Q_0 Q^{\gamma} \quad \text{implies} \quad Q_0 \subset Q^{\gamma} \subset Q^{2\gamma} \subset \dots \subset Q^{d\gamma} = Q_0\,,$$

hence $Q_0 = Q^{\gamma}$ which is a contradiction to the definition of d. [The case $Q^u \supset Q^v$ can be settled analogously.] $\square$

Let $E = E(P)$ be the set of all idempotents contained in $\overline{P}$. Then $E \subset Q_0 = P^r$. For, if $e \in E$, there is an $s, 1 \le s \le n_0$, such that $e \in P^s$. This implies $e = e^r \subset P^{rs} = Q_0$, hence $E \subset Q_0$.

Lemma 2

Suppose that $\overline{P}$ contains an identity element of $\overline{P}$, say e. Then

1) *$P^t \subset Q^t$ for any $t \ge 1$.*
2) *$e \in Q_0 = Q^d$, but none of the sets $Q, Q^2, \dots, Q^{d-1}$ contains e (if $d > 1$).*
3) *If s is the least integer for which $e \in P^s$, $1 \le s \le n_0$, then $d|s$. [Hence $d \le n_0$.]*
4) *$\hat{P} = \overline{P}$.*

Proof. 1) $P^t = P^t{\cdot}e \subset P^t{\cdot}Q_0 = Q^t$. 2) If $e \in Q^t$, then $e \in Q^t \subset Q^{2t} \subset \dots \subset Q^{dt} = Q_0$. By Lemma 1 $Q^t \subset Q_0$ implies $Q^t = Q_0$. 3) If $e \in P^s$, then $e \in Q^s = Q^d = Q_0$, hence d is a divisor of s. 4) $\overline{P} = P \cup P^2 \cup \dots \cup P^{n_0} \subset Q \cup Q^2 \cup \dots \cup Q^{n_0} = \hat{P} \subset \overline{P}$. $\square$

Proposition 3

Let S be a finite semigroup, $P \subset S$ and suppose that $\overline{P}$ contains an identity element (of $\overline{P}$). Then the following holds:

1) *$k(P) = \beta$, where $t = \beta$ is the least integer for which $|P^t| = |P^{t+1}|$.*
2) *$k(P) \le |Q_0| - |P| + 1$.*
3) *$|Q| = |Q^2| = \dots = |Q^d|$.*

Proof. Let $s \geq 1$ be the least integer such that $e \in P^s$ $(1 \leq s \leq n_0)$. Write $e = a_1 a_2 \dots a_s$ with all $a_i \in P$. For $t \geq 1$ we have

$$|P^t| = |P^t e| = |P^t a_1 a_2 \dots a_s| \leq |P^t a_1 \dots a_{s-1}| \leq \dots \leq |P^t a_1| \leq |P^t|\,.$$

Hence $|P^t| = |P^t a_1| \leq |P^{t+1}|$. Let β be the least integer for which $|P| < |P^2| < \dots < |P^{\beta-1}| < |P^\beta| = |P^{\beta+1}|$. We show that $|P^\beta| = |P^t|$ for all $t \geq \beta$.

Let $P = \{a_1, \dots, a_s, a_{s+1}, \dots, a_u\}$. Then $|P^\beta| = |P^{\beta+1}| = |\{P^\beta a_1 \cup P^\beta a_2 \cup \dots \cup P^\beta a_u\}|$. Since $|P^\beta| = |P^\beta a_1|$, we have $P^\beta a_j \subset P^\beta a_1$ for any $j \in \{1, 2, \dots, u\}$. This implies $\bigcup_{j=1}^u P^\beta a_j \subset P^\beta a_1$ and $P^{\beta+1} \subset P^\beta a_1 \subset P^{\beta+1}$, whence $P^{\beta+1} = P^\beta a_1$. Next for any $t \geq \beta$ we have $P^{t+1} = P^t a_1$, and since $|P^t a_1| = |P^t|$ (for any $t \geq 1$), $|P^{t+1}| = |P^t|$ (for any $t \geq \beta$). Since all sufficiently high powers have the same cardinality, the set $P^{\beta-1}$ does not belong to the periodic part of the sequence $\{P, P^2, P^3, \dots\}$. The set P^β belongs to the periodic part since $P^\beta = P^\beta e \subset P^{r+\beta}$ and $|P^\beta| = |P^{r+\beta}|$ imply $P^\beta = P^{r+\beta}$. Hence we have $k(P) = \beta$, and $|Q| = |Q^2| = \dots = |Q^d|$.
Next, P^β contains at least $|P| + \beta - 1$ different elements so that $|P| + \beta - 1 \leq |P^\beta| = |Q_0|$, whence $k(P) \leq |Q_0| - |P| + 1$. This proves Proposition 3. □

Remark. The identity $P^{k+1} = P^k a_1$ implies $P^{r+1} = P^r a_1$ i.e. $Q = Q_0 a_1$. Next $Q^2 = Q a_1 = Q_0 a_1^2$, $Q^3 = Q_0 a_1^3, \dots, Q^{d-1} = Q_0 a_1^{d-1}$. Hence $\hat{P} = \overline{P} = Q_0 \cup Q \cup \dots \cup Q^{d-1} = Q_0 \cup Q_0 a_1 \cup Q_0 a_1^2 \cup \dots \cup Q_0 a_1^{d-1}$.

Corollary 3

With the hypotheses of Proposition 3 there is an element $a \in P$ such that

$$\overline{P} = Q_0 \cup Q_0 a \cup Q_0 a^2 \cup \dots \cup Q_0 a^{d-1} = P^k \cup P^k a \cup P^k a^2 \cup \dots \cup P^k a^{d-1}\,.$$

Remark. Proposition 3 holds even in the non-commutative case. The assumption that $\overline{P}$ has an identity element is rather essential. The general case (without this assumption) is treated in [5]. Though $k(P) \leq |Q_0| - |P| + 1$ is true in any case, the statement $|Q^i| = |Q^j|$, $i \neq j$, need not hold.

EXAMPLE: Let us show on a simple example how this works.

Let S be the multiplicative semigroup of residue classes $\pmod{10}$. We represent the classes by integers $\{0, 1, \dots, 9\}$ and all calculations are $\pmod{10}$.

A) Choose $P = \{2, 3\}$. We have

$$P^2 = \{4, 6, 9\},\ P^3 = \{2, 7, 8\} \cdot |P^2| = |P^3| \quad \text{implies} \quad k(P) = 2$$

and all the following powers are of cardinality 3. We have $P^4 = \{1, 4, 6\}$. Since $1 \in P^4$, we conclude $d(P)|4$. Next $P^5 = \{2, 3, 8\}$, $P^6 = \{4, 6, 9\} = P^2$. Therefore $P^2 = P^6$. In our terminology $Q_0 = \{1, 4, 6\}$, $Q = \{2, 3, 8\}$, $Q^2 = \{4, 6, 9\}$, $Q^3 = \{2, 7, 8\}$.

Since $1 \equiv 3^4 \pmod{10}$, we may choose $a = 3$ and the decomposition of the Corollary has the form

$$\overline{P} = Q_0 \cup 3Q_0 \cup 9Q_0 \cup 7Q_0 \,.$$

Note finally, $|S| = 10$, while $|\overline{P}| = 8$. Note also that $Q_0 \cap Q = \emptyset$, while $Q_0 \cap Q^2 \neq \emptyset$.

B) Choose $P = \{2, 4\}$. Then $P^2 = \{4, 6, 8\}$, $P^3 = \{2, 4, 6, 8\} = \overline{P}$. Hence $P^3 = P^4$, $k(P) = 3$, $d(P) = 1$. Note that here there exists an identity element e of $\overline{P}$, namely $e = \{6\}$.

C) Choose $P = \{2, 5\}$. Then $P^2 = \{0, 4, 5\}$, $P^3 = \{0, 8, 5\}$, $P^4 = \{0, 6, 5\}$, $P^5 = \{0, 2, 5\}$, $P^6 = \{0, 4, 5\}$. Hence $P^2 = P^6$. Here $Q_0 = \{0, 6, 5\}$. Note that $\overline{P} = \{0, 2, 4, 6, 8, 5\} = P \cup P^2 \cup P^3 \cup P^4$ does not contain an identity element.

II. The group $G(p^\alpha)$

In this section we first prove a general statement concerning any finite group and then we shall restrict our attention to the group of residue classes $\pmod{p^\alpha}$ relatively prime to p, which will be denoted by $G(p^\alpha)$.

A.

Let G be a group with identity element e, $|G| = n$, and $P \subset G$. Then in the chain $e \subset Q_0 \subset \overline{P} \subset G$ all terms are groups. The decomposition $\overline{P} = Q_0 \cup Q_0 a \cup \ldots \cup Q_0 a^{d-1} = Q_0 \cup Q^1 \cup \ldots \cup Q^{d-1}$, shows that the Q^i, $1 \leq i \leq d$, are the cosets of Q_0 in $\overline{P}$. Hence they are mutually disjoint and $|Q^i| = |Q_0|$. Next $d = \frac{|\overline{P}|}{|Q_0|} \leq \frac{n}{|Q_0|}$. Also $k \leq |Q_0| - |P| + 1$. We have

$$k + d \leq \frac{n}{|Q_0|} + |Q_0| - |P| + 1 \,.$$

Since $1 \leq |Q_0| \leq n$ and $\frac{n}{|Q_0|} + |Q_0|$ has the largest value $n+1$ (which is attained for $|Q_0| = n$ and $|Q_0| = 1$), we have $k + d \leq n + 2 - |P|$.

Note that $d = n$ may occur if and only if P is a one point set, in which case $k = 1$ and $P = P^{n+1}$. Conversely, if P is a one point set, then $P = P^{d+1}$, where $d|n$.

If $|P| \geq 2$, then $k + d \leq n$, whence $k \leq n - 1$, $d \leq n - 1$.

Summarizing and using the result of Proposition 3 we have the following Proposition which holds for any finite group (even in the non-commutative case).

Proposition 4

Let G be a group, $|G| = n$, and $P \subset G$. Then (with $k = k(P)$, $d = d(P)$):

1) *The sets P^k, $P^{k+1}, \dots, P^{k+d-1}$ are pairwise disjoint and all of the same cardinality.*
2) *If β is the least integer for which $|P^\beta| = |P^{\beta+1}|$, then $k(P) = \beta$. In any case $k \le |P^r| - |P| + 1$.*
3) *$d = \frac{|\overline{P}|}{|P^r|} \le \frac{n}{|P^r|}$ and $d|n$.*
4) *$k + d \le n + 2 - |P|$.*

Remark. The first part of these statements goes back to *Frobenius* [3].

B.

We now turn to the study of $G(p^\alpha)$. We have $\left|G(p^\alpha)\right| = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Denote $n = \varphi(p^\alpha)$.

If $|P| = 1$, then $k(P) = 1$, $d(P)|\varphi(p^\alpha)$ and $P = P^{1+\varphi(p^\alpha)}$.

Suppose in what follows $|P| \ge 2$. Then $k \le |P^r| - 1$, hence $|P^r| \ge k + 1$ and $d = \frac{|\overline{P}|}{|P^r|} \le \frac{n}{k+1}$ (and, of course, $d|n$). Since d is an integer, we may write $d \le \left[\frac{n}{k+1}\right]$, where $[x]$ denotes the "integral part" of x.

Also $k + d \le n$ implies $d \le n - 1$ and since $d|n$, we have $d\Big|\frac{n}{2}$, hence $d \le \frac{1}{2}n$.

We now consider two cases.

a) If $k > \frac{n}{2}$, then $d \le \frac{n}{\frac{n}{2}+1} < 2$, hence $d = 1$, so that $P^k = P^{k+1}$ and since $k \le |P^r| - 1 \le n - 1$, we have $P^{n-1} = P^n$. (Below we shall show that this case may occur.)
b) Suppose $k \le \frac{n}{2}$. Then $k + d \le k + \left[\frac{n}{k+1}\right]$. For $1 \le k \le \frac{n}{2}$ the term to the right has the largest value $\frac{n}{2} + 1$ (which is attained for $k = 1$ and $k = \frac{n}{2}$). Hence $k + d \le \frac{n}{2} + 1$, $k \le \frac{n}{2} + 1 - d(P)$ and $P^{\frac{n}{2}+1-d} = P^{\frac{n}{2}+1}$, where d divides $\frac{n}{2}$. Multiplying by P^{d-1} we get $P^{n/2} = P^{n/2+d}$ and (independently of P and d) $P^{n/2} = P^n$.

We have proved:

Proposition 5

Let $P \subset G(p^\alpha)$, $n = \varphi(p^\alpha)$.

a) *If $k(P) \ne n - 1$, then $k(P) \le \frac{n}{2}$.*
b) *If $|P| = 1$, then $P = P^{n+1}$.*
c) *If $|P| \ge 2$, then either $P^{n-1} = P^n$ or $P^{n/2} = P^n$.*

To get an universal formula (in the sense of the introduction) note that each of the identities $P = P^{n+1}$, $P^{n-1} = P^n$, $P^{\frac{n}{2}} = P^n$ (multiplied by a suitable power of P) implies $P^{n-1} = P^{2n-1}$.

Remark 1. In the case b), i.e., $|P| \geq 2$, $k(P) \leq \frac{n}{2}$, we can get in *any concrete case* a stronger result (i.e., with smaller exponents). We have seen that in this case $P^{\frac{n}{2}+1-d(P)} = P^{\frac{n}{2}+1}$ $(1 \leq d(P) \leq \frac{n}{2})$. Unfortunately, since $d(P)$ depends on P, this result cannot serve as a starting-point to find an universal formula.

Remark 2. In the proof of Proposition 5 we have not used that $G(p^\alpha)$, $p \neq 2$, is a cyclic group. Hence it holds also for $p = 2$, in which case if $\alpha \geq 3$ the group is not cyclic. But in this case, using the known structural properties of $G(2^\alpha)$, we immediately obtain:

a) If $|P| = 1$, then $P = P^{\frac{n}{2}+1}$. b) If $|P| \geq 2$ and $k(P) > \frac{n}{4}$, then $P^{\frac{n}{2}} = P^{\frac{n}{2}+1}$. c) If $|P| \geq 2$ and $k(P) \leq \frac{n}{4}$, then $P^{\frac{n}{4}} = P^{\frac{n}{2}}$. This implies that for any $P \subset G(2^\alpha)$, $\alpha \geq 3$, we have $P^{\frac{n}{2}} = P^n$.

The following is a universal formula of Euler-Fermat type for subsets of $G(p^\alpha)$.

Theorem 6

Let P be a subset of $G(p^\alpha)$ and $n = \varphi(p^\alpha)$.

a) If p is an odd prime, then $P^{n-1} = P^{2n-1}$.

b) If $p = 2$, then $P^{\frac{n}{2}} = P^n$.

Example: Suppose $p \neq 2$. Then the group $G(p^\alpha)$ is a cyclic group of order $n = \varphi(p^\alpha)$. If g is a primitive element $\pmod{p^\alpha}$, we may write $G(p^\alpha) = \{g, g^2, \ldots, g^n = 1\}$.

a) Choose $P = \{1, g\}$. Then $P^2 = \{1, g, g^2\}, \ldots, P^{n-1} = \{1, g, \ldots, g^{n-1}\}$ and $P^n = P^{n-1}$. Hence $k(P) = n-1$ and $d(P) = 1$. This shows that the case $P^n = P^{n-1}$ cannot be omitted.

b) We show that to any divisor h of $n = \varphi(p^\alpha)$ *there is a subset* $P \subset G(p^\alpha)$ such that $d(P) = h$. Write $n = h \cdot \ell$ and consider the set $P = g\{1, g^h\}$. Then $P^2 = g^2\{1, g^h, g^{2h}\}, \ldots, P^{\ell-1} = g^{\ell-1} \cdot \{1, g^h, \ldots, g^{(\ell-1)h}\}$ and $P^\ell = g^\ell\{1, g^h, \ldots, g^{(\ell-1)h}\}$. This implies $|P^{\ell-1}| = |P^\ell|$, hence $k(P) = \ell - 1$.

Denote $\{1, g^h, \ldots, g^{(\ell-1)h}\} = H$. Then H is subgroup of $G(p^\alpha)$, and $P^{\ell-1} = g^{\ell-1}H$, $P^\ell = g^\ell H, \ldots, P^{\ell-1+h} = g^{\ell-1} \cdot g^h H = g^{\ell-1}H$. This implies $P^{\ell-1} = P^{\ell-1+h}$, hence $d(P)|h$. Now $\hat{P} = g^{\ell-1}H \cup g^\ell H \cup \ldots \cup g^{\ell+h-2}H = g^{\ell-1}\{1 \cup g \cup \ldots \cup g^{h-1}\} \cdot \{1 \cup g^h \cup \ldots \cup g^{(\ell-1)h}\}$. The product of the brackets is exactly the set $G(p^\alpha)$, so that $|\hat{P}| = h \cdot \ell = n$ and by Proposition 4 $d(P) = \frac{|\hat{P}|}{|P^{\ell-1}|} = \frac{h \cdot \ell}{\ell} = h$.

III. The semigroup $S(p^\alpha)$

The semigroup $S(p^\alpha)$, $p^\alpha > 2$, can be written as a union of disjoint sets $S(p^\alpha) = G \cup N$, where $G = G(p^\alpha)$ and $N = p\,G \cup p^2 G \cup \ldots \cup p^{\alpha-1} G \cup \{0\}$.

1) If $P \subset N$, then $P^\alpha = \{0\}$, hence $k(P) \leq \alpha$, $d(P) = 1$.

2) If $P \subset G(p^\alpha)$, then we have seen that always $P^{m-1} = P^{2m-1}$, where $m = \varphi(p^\alpha)$. (The notation $m = \varphi(p^\alpha)$ will be used only in this section.)

3) Suppose finally that $P = P_1 \cup N_1$, where $P_1 = G \cap P \neq \emptyset$ and $N_1 = N \cap P \neq \emptyset$. We have

$$P^\alpha = (P_1 \cup N_1)^\alpha = P_1^\alpha \cup P_1^{\alpha-1} N_1 \cup \ldots \cup P_1 N_1^{\alpha-1} \cup \{0\}\,,$$

and for any $t \geq 1$

$$P^{\alpha+t} = P_1^{\alpha+t} \cup P_1^t \cdot \{P_1^{\alpha-1} N_1 \cup P_1^{\alpha-2} N_1^2 \cup \ldots \cup P_1 N_1^{\alpha-1} \cup 0\}\,.$$

Denote the bracket to the right by M. We have

$$P^{\alpha+t} = P_1^{\alpha+t} \cup P_1^t \cdot M\,, \quad \text{where} \quad M \quad \text{does not depend on } t\,.$$

Put in $t = k(P_1) + d(P_1) - 1 \geq 1$. Then $P^{\alpha+k(P_1)+d(P_1)-1} = P_1^{\alpha+k(P_1)+d(P_1)-1} \cup P_1^{k(P_1)+d(P_1)-1} \cdot M = P_1^{\alpha-1+k(P_1)} \cup P_1^{k(P_1)-1} \cdot M = P^{\alpha+k(P_1)-1}$. Hence $P^{\alpha+k(P_1)-1+d(P_1)} = P^{\alpha+k(P_1)-1}$. By definition $P^{k(P)} = P^{k(P)+d(P)}$. Hence $k(P) \leq \alpha + k(P_1) - 1$ and $d(P)|d(P_1)$. We prove that $d(P) = d(P_1)$. Denote $\tau = \alpha + k(P_1) - 1$. Then $P^\tau = P_1^\tau \cup M \cdot P_1^{\tau-\alpha}$ and $P^{\tau+d(P)} = P_1^{\tau+d(P)} \cup M \cdot P_1^{\tau-\alpha+d(P)}$. Since both $M \cdot P_1^{\tau-\alpha}$ and $M P_1^{\tau-\alpha+d(P)}$ are contained in N, we have $P_1^\tau = P_1^{\tau+d(P)}$, so that $d(P_1)|d(P)$ and $d(P) = d(P_1)$.

We now use the considerations which have led to Proposition 5.

a) If $|P| = 1$, then $k(P_1) = 1$, and $d(P_1)/m$. Hence $k(P) \leq \alpha + k(P_1) - 1 = \alpha$, and $d(P)|\varphi(p^\alpha)$, so that we have $P^\alpha = P^{\alpha+m}$. If $p = 2$, we have $P^\alpha = P^{\alpha+\frac{m}{2}}$.

b) Suppose $|P_1| \geq 2$ and $k(P_1) > \frac{m}{2}$, $p =$ odd. We have proved that $k(P_1) = m - 1$ and$d(P_1) = 1$. In what follows we may suppose $M \geq 2$ (and $\alpha \geq 2$), since otherwise S is a group with zero and Proposition 5 implies $P^{m-1} = P^m$.

Having in mind $P^{m-1} = P_1^{m-1} \cup M P_1^{m-1-\alpha}$ (for $m - 1 \geq \alpha$), we shall consider the sequence $\{M, MP_1, MP_1^2, \ldots\}$. Let $P_1 = \{a_1, \ldots, a_s\}$. Then (with $MP^\circ = M$) we have

$$MP_1^{i+1} = MP_1^i\{a_1, \ldots, a_s\} = \{MP_1^i a_1 \cup \ldots \cup MP^i a_s\}\,.$$

Since for any $A \subset M \subset N$, we have $|A\,a_j| = |A|$, we conclude $|MP_1^{i+1}| \geq |MP_1^i|$, so that $|M| \leq |MP_1| \leq |MP_1^2| \leq \ldots$.

Let l be the least integer such that $MP_1^l = MP_1^{l+1}$. (Such an l exists, since $P_1^{m-1} = P_1^m$ implies $MP_1^{m-1} = MP_1^m$.) We have

$$|M| < |MP_1| < \ldots < |MP_1^{l-1}| < |MP_1^l| = |MP_1^{l+1}| .$$

Clearly $|MP_1^l| \geq l+2$, and $l+2 \leq |MP_1^l| \leq |N| = p^{\alpha-1}$. Hence $l \leq p^{\alpha-1} - 2$. Now for any odd prime p, we have $p^{\alpha-1} - 2 \leq \varphi(p^\alpha) - 1 - \alpha$. Denoting $L = p^{\alpha-1} - 2$, this means $MP_1^L = MP_1^{L+1} = MP_1^{L+2} = \ldots$, in particular, $P^{m-1} = P_1^{m-1} \cup MP_1^L$ and $P^m = P_1^m \cup MP_1^L$, whence $P^{m-1} = P^m$.

If $p = 2$, $\alpha \geq 3$, we use the identity $P^{\frac{m}{2}+\alpha} = P_1^{\frac{m}{2}+\alpha} \cup MP_1^{\frac{m}{2}}$. Since both $P_1^{\frac{m}{2}}$ and $P_1^{\frac{m}{2}+\alpha}$ are contained in the periodic part of the sequence $\{P_1, P_1^2, P_1^3, \ldots\}$, and $d(P_1)|\frac{m}{2}$, we have $P^{\frac{m}{2}+\alpha} = P^{m+\alpha}$. (Note, in particular, that $k(P) \leq \frac{m}{2} + \alpha$.)

c) Suppose $|P_1| \geq 2$ and $k(P_1) \leq \frac{m}{2}$. Then $k(P) \leq \alpha - 1 + k(P_1)$. In this case we have seen that $k(P_1) + d(P_1) \leq \frac{m}{2} + 1$. Hence $k(P_1) \leq \frac{m}{2}$, and $d(P_1)\big|\frac{m}{2}$, so that $d(P)\big|\frac{m}{2}$. Therefore $P^{\alpha-1+\frac{m}{2}} = P^{\alpha-1+m}$. For a prime $p \geq 3$ we have $\alpha - 1 + \frac{1}{2}\varphi(p^\alpha) \leq \varphi(p^\alpha) - 1$, so that $P^{m-1} = P^{\frac{3}{2}m-1}$.

In the case $p = 2$ (in which case $P_1^{\frac{m}{4}} = P_1^{\frac{m}{2}}$) we use the identity $P^{\alpha+\frac{m}{4}} = P_1^{\alpha+\frac{m}{4}} \cup MP_1^{\frac{m}{4}}$. Here both $P_1^{\alpha+\frac{m}{4}}$ and $P_1^{\frac{m}{4}}$ are elements of the periodic part of the sequence $\{P_1, P_1^2, \ldots\}$, so that $P^{\alpha+\frac{m}{4}} = P^{\alpha+\frac{3}{4}m}$.

To get a formula comprising the three cases a), b), c), note that each of the identities $P^\alpha = P^{\alpha+m}$, $P^{m-1} = P^m$, and $P^{m-1} = P^{\frac{3}{2}m-1}$ (multiplied by a suitable power of P) implies $P^{m-1} = P^{2m-1}$.

In the case $p = 2$ the three identities $P^\alpha = P^{\alpha+\frac{m}{2}}$, $P^{\alpha+\frac{m}{2}} = P^{\alpha+m}$, $P^{\alpha+\frac{m}{4}} = P^{\alpha+\frac{3}{4}m}$ are covered by $P^{\alpha+\frac{m}{2}} = P^{\alpha+m}$.

We have proved

Theorem 7

Let P be a subset of $S(p^\alpha)$, and $m = \varphi(p^\alpha)$.
We have

a) If p is an odd prime, then $P^{m-1} = P^{2m-1}$.

b) If $p = 2$, then $P^{\frac{m}{2}+\alpha} = P^{m+\alpha}$.

This is a universal formula of Euler–Fermat type for subsets of $S(p^\alpha)$.

If $G \cap P \neq \emptyset$, then some power of P contains the element 1 and $1 \in \overline{P}$. By Proposition 3 we have (with $k = k(P)$) $|P^k| = |P^{k+1}| = \ldots = |P^{k+d-1}|$. By Proposition 4 this holds also if $P \subset G$ and trivially if $P \subset N$.

Corollary 7

If $P \subset S(p^\alpha)$ and $k = k(P)$, $d = d(P)$, we have $|P^k| = |P^{k+1}| = \ldots = |P^{k+d-1}|$. Also $k(P)$ is equal to the least integer β for which $|P^\beta| = |P^{\beta+1}|$.

Remark. Note explicitly that if $P \cap N \neq \emptyset$, then the sets P^k, $P^{k+1} \ldots$ are not mutually disjoint. Also $\hat{P} = \overline{P}$ need not hold.

IV. The general case

We finally treat the case $S(m)$, where $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, $(\alpha_i \geq 1)$ is the canonical factorization of $m > 2$ into distinct prime powers.

We shall use the known fact that

$$S(m) \approx S(p_1^{\alpha_1}) \times S(p_2^{\alpha_2}) \times \ldots \times S(p_s^{\alpha_s})\,.$$

Suppose in the following that $p_1 < p_2 < \ldots < p_s$. We have, of course, $S(p_i^{\alpha_i}) \cap S(p_j^{\alpha_j}) = \emptyset$ for $i \neq j$. The isomorphism can be realized by assigning to any $a \in S(m)$ an s-tuple $< a_1, a_2, \ldots, a_s >$, where $a_i \equiv a \text{mod} p_i^{\alpha_i}$.

If $a \in S(m) \mapsto \langle a_1, a_2, \ldots, a_s \rangle$, $b \in S(m) \mapsto \langle b_1, b_2, \ldots, b_s \rangle$, then $ab \in S(m) \mapsto \langle a_1 b_1,\, a_2 b_2, \ldots, a_s b_s \rangle$.

No misunderstanding can arise if we denote the elements of $S(p^\alpha)$ by $\{1, 2, 3, \ldots, p^\alpha = 0\}$ for each p. The position in the s-tuple indicates that, e.g., a_2 is an element of $S(p_2^{\alpha_2})$.

For instance: Let $m = 1575 = 3^2 \cdot 5^2 \cdot 7$. If $a = 39 \in S(1575)$, then $a \mapsto \langle 3, 14, 4 \rangle$. If $b = 100 \in S(1575)$, then $b \mapsto \langle 1, 0, 2 \rangle$. If $c = 1 \in S(1575)$, then $c \mapsto \langle 1, 1, 1 \rangle$. Next, if $P = \{39, 100, 1\}$ is a subset of $S(m)$, then $P \mapsto \big\{ \langle 3, 14, 4 \rangle,\, \langle 1, 0, 2 \rangle,\, \langle 1, 1, 1 \rangle \big\}$.

Suppose now that $P \subset S(m)$, $|P| = t$ and

$$P \mapsto \big\{ \langle a_1^{(1)}, a_2^{(1)}, \ldots, a_s^{(1)} \rangle\,,\, \langle a_1^{(2)}, a_2^{(2)}, \ldots, a_s^{(2)} \rangle, \ldots,\, \langle a_1^{(t)}, a_2^{(t)}, \ldots, a_s^{(t)} \rangle \big\}\,.$$

We define $P_i = \big\{ a_i^{(1)}, a_i^{(2)}, \ldots, a_i^{(t)} \big\} \subset S(p_i^{\alpha_i})$.

For any $\tau \geq 1$ we have

$$P^\tau \mapsto \big\{ \langle a_1^{(1)}, \ldots, a_s^{(1)} \rangle, \ldots, \langle a_1^{(t)}, \ldots a_s^{(t)} \rangle \big\}^\tau\,.$$

The i-th coordinate of any term of the product is an element of $S(p_i^{\alpha_i})$. The union of all i-th coordinates is exactly the set $\big\{ a_i^{(1)}, a_i^{(2)}, \ldots, a_i^{(t)} \big\}^\tau$ hence equal to P_i^τ.

Now consider the sequence $\{P_i, P_i^2, P_i^3, \ldots\} \subset S(p_i^{\alpha_i})$. By Theorem 7 we have: a) If $p_i \geq 3$, $k(P_i) \leq \varphi(p_i^{\alpha_i}) - 1$, and $d(P_i) \big| \varphi(p_i)$. b) If $p_1 = 2$, $k(P_1) \leq \alpha_1 + \frac{1}{2}\varphi(2^{\alpha_i})$ and $d(P_1) \big| \frac{1}{2}\varphi(2^{\alpha_1})$.

Denote $k^* = \max\{\alpha_1 + \frac{1}{2}\varphi(2^{\alpha_1}),\, \varphi(p_i^{\alpha_i}) - 1 \mid i = 1, \ldots, s\}$, with the convention that the first term appears if and only if m is even. Next, denote d^*=l.c.m.

$[\varphi(p_1^{\alpha_1}),\ \varphi(p_2^{\alpha_2}),\dots,\varphi(p_s^{\alpha_s}]$, with the convention that for even m we replace $\varphi(2^{\alpha_1})$ by $\frac{1}{2}\varphi(2^{\alpha_1})$. Then for any $P_i \subset S(p_i^{\alpha_i})$ we have $P_i^{k^*} = P_i^{k^*+d^*}$ $(i = 1, 2, \dots s)$. Moreover

$$|P_i^{k^*}| = |P_i^{k^*+1}| = \dots = |P_i^{k^*+d^*-1}|\,.$$

This implies

$$P^{k^*} = P^{k^*+d^*} \quad \text{and} \quad |P^{k^*}| = |P^{k^*+1}| = \dots = |P^{k^*+d^*-1}|\,.$$

The last statement follows from the fact that $P_i^{k^*} \cap P_j^{k^*} = \emptyset$ if $i \neq j$.

[Note that in our assignment $P^{k^*} \mapsto T$, T contains $|P^{k^*}|$ *specified* s-tuples. Each member of T and T as a whole is contained in the periodic part of the sequence $\{P, P^2, \dots\}$ (described by s-tuples). We have $T \subset P_1^{k^*} \times P_2^{k^*} \times \dots \times P_s^{k^*}$, but – in general – T is only a proper subset of $P_1^{k_1^*} \times \dots \times P_s^{k^*}$ (and not the whole product).]

Summarizing we have

Theorem 8

Let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, $p_1 < p_2 < \dots < p_s$, p_i different primes, $\alpha_i \geq 1$. Denote $k^* = \max\{\alpha_1 + \frac{1}{2}\varphi(2^{\alpha_1}),\ \varphi(p_i^{\alpha_i}) - 1 \mid i = 1, \dots, s\}$, with the convention that the first term appears if and only if m is even. Then for any subset $P \subset S(m)$, we have $P^{k^*} = P^{k^*+d^*}$, where $d^* = l.c.m..\ \big[\varphi(p_1^{\alpha_1}), \dots, \varphi(p_s^{\alpha_s})\big]$, with the convention that $\varphi(2^{\alpha_1})$ is replaced by $\frac{1}{2}\varphi(2^{\alpha_1})$ if m is even.

Moreover, $|P^{k^*}| = |P^{k^*+1}| = \dots = |P^{k^*+d^*-1}|$ and k^* is the least integer β for which $|P^{\beta}| = |P^{\beta+1}|$.

Example: To have a numerical illustration, consider the semigroup $S(1575) = S(3^2 \cdot 5^2 \cdot 7)$. We have $k^* = \max\big\{\varphi(3^2) - 1,\ \varphi(5^2) - 1,\ \varphi(7) - 1\big\} = \max\{5, 19, 5\} = = 19$, $d^* = l.c.m.\big[\varphi(3^2),\ \varphi(5^2),\ \varphi(7)\big] = l.c.m.[6, 20, 6] = 60$. Hence, for any subset $P \subset S(1575)$, we have $P^{19} = P^{79}$.

References

1. P. Dubreil, Fragmented rings, *Proc. Royal Soc. of Edinburgh* **78A** (1978), 273–283.
2. P. Dubreil, Semigroups and rings, *Proc. Royal Soc. of Edinburgh* **78A** (1978), 257–264.
3. G. Frobenius, Über endliche Gruppen, *Sitzungsber. Akad. Wiss. Berlin* (1895), 163–194.
4. Š. Schwarz, The role of semigroups in the elementary theory of numbers, *Math. Slovaca* **31** (1981), 369–395.
5. Š. Schwarz, Powers of subsets in a finite semigroup, Semigroup Forum, (to appear).