ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1999
Seria: MATEMATYKA-FIZYKA z. 84 Nr kol. 1411

Piotr R. KASPRZYK

ROOTS OF PERMUTATIONS

Summary. Criteria for existence of roots of order n for a given permutation are found. It is done by analyzing its cycle decomposition. Our results are generalizations of known cases for n being either prime or a product of two primes.

PIERWIASTKOWANIE PERMUTACJI

Streszczenie. W dokumencie tym opisane są kryteria pierwiastkowalności permutacji w stopniu n. W celu ich znalezienia analizuje się rozkład permutacji na cykle. Przedstawiane wyniki są uogólnieniem znanych rozwiązań dla n będącego liczbą pierwszą lub iloczynem dwóch liczb pierwszych.

1. Separating divisor

In this paper $\mathbf{N}$ denotes the set of all natural numbers. Let $n \in \mathbf{N}$. For each $m \in \mathbf{N}$ we consider the set:

$$S_{m,n} = \{x \in \mathbf{N} : (n/x, m) = 1\}.$$

Lemma 1. *Let m and n be as above. If $x, y \in S_{m,n}$ then $(x, y) \in S_{m,n}$.*

Proof. Let $d = (x, y)$, $x = dx'$, $y = dy'$, $(x', y') = 1$. Since by assumption $(n/x, m) = 1$ we get $(n/x \cdot x', m)|x'$. Similarly $(n/y' \cdot y', m)|y'$. So $(n/d, m)|(x', y')$ and hence $(n/d, m) = 1$.∎

Corollary 1. *Every $x \in S_{m,n}$ is a multiple of d_m where d_m is the smallest element in $S_{m.n}$.*

Further in this note we shall call d_m the *divisor separating n from m.*

2. Cycles and their n-th powers

We consider first the n-th powers of permutations. Every permutation can be presented as a product of disjoint cycles. We consider the n-th powers of these cycles.

Proposition 2. *The n-th power of a cycle of the length l is a product of (l, n) cycles of the length $l/(l, n)$.*

Proof. We consider a cycle $(0, 1, \ldots, l-1)$. The cycle can be referred to as a function:

$$c(x) = x + 1 (\mathrm{mod}\ l), x = 0, \ldots, l-1,$$

n-th power of this cycle is a function

$$d(x) = x + n.$$

The function is the permutation which is a product of cycles of the length m where m is the smallest such that:

$$d^m(x) = x.$$

This leads to:

$$x + mn = x,$$

and finally

$$mn = 0(\text{mod } l).$$

Hence $mn = kl$ for a positive k. Note that $mn = [l, n]$. Indeed $n|mn$ and $l|mn$ and if there existed $k' < k$ for which $m'n = k'l$, it would lead to $d^{m'}(x) = x$ with $m' < m$ despite assumption that m is the smalest natural number satisfying above condition. Hence $mn = [l, n]$. So $m = [l, n]/n = ln/(l, n)n = l/(l, n)$. We proved that the length of every cycle (cycle containing any x) is $l/(l, n)$. Since each of l x's belongs to a cycle, their number is $l/(l/(l, n)) = (l, n)$.∎

3. Criteria for existence of roots for permutations

A permutation σ *has an n-th root* if there exists a permutation π, for which $\pi^n = \sigma$.

Theorem 3. *A permutation σ has an n-th root if and only if the number of cycles of the length m in σ is a multiple of the divisor d_m separating n from m.*

Proof.

1. Assume that permutation σ has a root π. Let there exist cycles of length m in decomposition of σ. Then in π there exists at least one cycle of the length l_i, for which (by Proposition 2.):

$$l_i/(l_i, n) = m.$$

We denote $k_i := (l_i, n)$ then $l_i = mk_i$. Every cycle of the length mk_i in π provides (n, mk_i) cycles in σ. Since $(n, mk_i) = (n, l_i) =: k_i$ we get $(n/k_i, m) = 1$, so $k_i \in S_{m,n}$ (see section 1.). So k_i is a multiple of d_m. Number of all cycles of the length m in σ is equal $\sum k_i$, so it is also divisible by d_m.
2. Assume that for every m number of cycles of the length m is equal kd_m. Thus we can group them into sections of d_m cycles. For every such a group there exists a cycle of the length md_m which is a root of the group. Indeed, for a group:

$$(c_{11}, \ldots, c_{1m})(c_{21}, \ldots, c_{2m}) \cdots (c_{d_m 1}, \ldots, c_{d_m m})$$

this cycle is for example:

$$(c_{11}, c_{21}, \ldots, c_{d_m 1}, c_{12}, c_{22}, \ldots, c_{d_m 2}, c_{1m}, c_{2m}, \ldots, c_{d_m m}).$$

(The cycle of the length md_m to the n-th power gives (n, md_m) cycles. As $(n/d_m, m) = 1$ we have $(n, md_m) = d_m$. Thus the group of d_m cycles of the length m is the n-th power of a cycle of the length md_m.)∎

4. Examples

1. $n = p$

If n is a prime then $d_m \neq 1$ only for $m = kp$. And then $d_m = p$. In this case a permutation can have only p-th root, and it has it if and only if the number of its cycles of the length kp is divisible by p. The number of cycles of other lengths should be divisible by 1, so it is not important.

2. $n = pq$

In this case $d_m \neq 1$ only for $m = kp$, $m = lq$, and $m = xpq$. The latter implies $d_m = pq = n$, and the first two (assuming that k is not a multiple of p, and l is not a multiple of q) imply $d_m = p$ and $d_m = q$.

3. $n = p^a$

Just like **1.**, except that $d_m = p^a = n$ for $m = kp$. It implies that a permutation has a p^a-th root if and only if the number of its cycles of the length kp is divisible by p^a.

4. $n = p^a q^b$

Like **2.**: $d_m = p^a q^b = n$ for $m = xpq$, $d_m = p^a$ for $m = kp$ and $d_m = q^b$ for $m = lq$. (Assume that that k is not a multiple of p, l is not a multiple of q.)

In general case the procedure is similiar.

5. Notes

Problem of determining if a permutation has a root was analysed before. Two first cases of the previous section were studied by P. Gawron [2, 3]. Another approach to general case can be found in paper [4] by S. Łojasiewicz.

References

1. W. Sierpiński, *Teoria Liczb,* PWN, Warszawa 1959.

2. P. Gawron, *O poszukiwaniu pierwiastka w grupie bijekcji,* I Sesja SKN Wydz. Mat.-Fiz. Pol. Śl.

3. P. Gawron, *Rozwiązanie równania* $f^n = q$ *w grupie bijekcji,* Zesz. Nauk. Pol. Śl. Mat.-Fiz. **35** (1979), 7-9.

4. S. Łojasiewicz, *Solution générale de l'équation fonctionelle* $f(f(\ldots f(x)\ldots)) = g(x)$, Annal. Pol. Math. **XXIV**, t. 1 (1951), 88-91.

Piotr R. Kasprzyk
Institute of Mathematics
Silesian Technical University
Kaszubska 23
44-100 Gliwice

Streszczenie

W artykule znalezione kryteria pierwiastkowalności permutacji. Celem ich znalezienia analizuje się zachowanie pojedynczego cyklu przy podnoszeniu go do n-tej potęgi i ilość nowych cykli w ten sposób otrzymaną. Następnie całą permutację traktuje się jako iloczyn cykli i na podstawie poprzednich rozważań wysuwa się wnioski ogólne. Artykuł zawiera także kilka przykładów przypadków szczególnych, w których określenie, czy permutacja jest pierwiastkowalna, jest prostsze. Są to między innymi znane wcześniej przypadki n będącego liczbą pierwszą lub iloczynem dwóch liczb pierwszych.