AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **49** (2011), Pages 265–272

A combinatorial generalization of Wilson's theorem

Szilárd András*

Babeş-Bolyai University
Cluj Napoca
Romania
andraszk@yahoo.com

Abstract

Consider all possible oriented Hamiltonian cycles over the vertices of a regular n-gon, where $n \in \mathbb{N}$, $n \geq 3$. The main aim of this note is to count the cycles which are not equivalent under the rotations of the n-gon. It is well known when n is a prime number the number of simple cycles is

$$|HC_n| = n - 2 + \frac{(n-1)! + 1}{n},$$

so the above counting problem leads to the classical Wilson's theorem. We count the nonequivalent cycles for the case of an arbitrary natural number n, so the obtained congruences can be viewed as natural generalizations of Wilson's theorem. The same results were obtained recently by T.J. Evans using the Burnside theorem for counting the number of orbits of a group action. Our method uses an argument by function iteration and leads to some additional congruences.

1 Introduction

The classical theorem of Wilson has several different proofs (see [3], [2]). One of the proofs is based on a simple counting argument. For a prime number p the directed Hamiltonian cycles on the vertices of a regular p-gon can be classified into 2 classes as follows: one of the classes contains cycles which are invariant under rotations of angle $2k\pi/p$ ($k \in \mathbb{N}$); the elements of the second class form sets of size p such that in every set the cycles can be obtained from an arbitrary element of this set by rotating it by $2\pi/p$, $4\pi/p, \ldots, 2(p-1)\pi/p, 2\pi$ around the center of the p-gon. In other words, if we denote by C_p the set of all oriented Hamiltonian cycles and we call $x, y \in C_p$ equivalent if and only if x can be obtained from y by a rotation of angle

$$\alpha \in \{2\pi/p, 4\pi/p, \ldots, 2(p-1)\pi/p,\ 2\pi\},$$

* The author was supported by the Hungarian University Federation of Cluj Napoca.

around the center of the p-gon, then $(p-1)$ equivalence classes contain 1 cycle (these correspond to the regular convex and regular star polygons) and all other classes contain p elements, so the total number of equivalence classes is

$$|HC_p| = p - 1 + \frac{(p-1)! - (p-1)}{p}.$$

It follows that p divides $(p-1)! + 1$, which is Wilson's Theorem.

In order to generalize this argument we rephrase the counting problem in terms of iterated functions, periodic points and orbits. If $f : C_n \to C_n$ is the rotation of angle $2\pi/n$, then the rotation of angle $2k\pi/n$ is $f^k = \underbrace{f \circ f \circ \ldots \circ f}_{k}$, so every cycle is a fixed point of the operator f^n. If $x \in C_n$, the orbit of x contains the cycles which can be obtained from x by rotations of angle $2k\pi/n$, $k \in \mathbb{N}$:

$$\{x, f(x), f^2(x), \ldots\},$$

hence the number of nonequivalent cycles is the number of periodic orbits associated to the fixed points of f^n. In the next section we recall some known results regarding the counting of periodic points and orbits. We use a number theoretic approach in deducing the basic relations to emphasize the equivalence between two types of congruencies (see [11], Möbius inversion counting), one involving the Möbius function and the other the Euler function. Our results can be obtained also by using the Pólya-Burnside enumeration theory (see [10]).

2 Preliminary results

For a set X and a function $f : X \to X$ we denote by F_f the set of fixed points of f and by $P_f(d)$ the set of periodic points of f with period d. One can observe that if $x \in X$ is a fixed point of f^n, than the period of x is a divisor of n. This and the Möbius inversion formula implies the following theorem.

Theorem 1. *If $f : X \to X$ is a function and f^n has finitely many fixed points, then*

a) $F_{f^n} = \bigcup_{d|n} P_f(d)$;

b) $|F_{f^n}| = \sum_{d|n} |P_f(d)|$;

c) $|P_f(n)| = \sum_{d|n} \mu\left(\frac{n}{d}\right) |F_{f^d}|$, *where μ is the Möbius function.*

If x is a periodic point with period n, than the elements $f(x), f^2(x), \ldots, f^{n-1}(x)$ also have period n, so $|P_f(n)| \equiv 0 (\text{mod } n)$. This implies the following congruence relation:

Corollary 1. *If $f : X \to X$ and the set $P_f(n)$ is finite, then*

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) |F_{f^d}| \equiv 0 (\text{mod } n). \tag{1}$$

Theorem 2. *If $f : X \to X$ and the set F_{f^n} is finite, then*

$$n \cdot F(n) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) \cdot \left|F_{f^d}\right|, \tag{2}$$

where $F(n)$ denotes the number of periodic orbits corresponding to the fixed points of f^n and φ is the Euler function.

Remark 1. This result appears in [6] as Lemma 1 and is derived from the Burnside theorem. In what follows we give an alternative proof.

Proof. If x is a periodic point with period d, then the points $f(x), f^2(x), \cdots, f^{d-1}(x)$ are all of period d, hence the number of periodic orbits with length d is $\frac{1}{d} \cdot |P_f(d)|$ and so we have

$$F(n) = \sum_{d|n} \frac{1}{d} \cdot |P_f(d)|.$$

Using the Gauss identity for the Euler function $m = \sum_{d|m} \varphi(d)$ we obtain

$$\begin{aligned} n \cdot F(n) &= \sum_{d|n} \frac{n}{d} |P_f(d)| \\ &= \sum_{d|n} \left(\sum_{d_1 | \frac{n}{d}} \varphi\left(\frac{n}{d \cdot d_1}\right) \right) \cdot |P_f(d)| \\ &= \sum_{d|n} \sum_{d_1 | \frac{n}{d}} \varphi\left(\frac{n}{d \cdot d_1}\right) \cdot |P_f(d)| \\ &= \sum_{d|n} \left(\varphi\left(\frac{n}{d}\right) \sum_{d_1|d} |P_f(d_1)| \right) \\ &= \sum_{d|n} \varphi\left(\frac{n}{d}\right) \cdot \left|F_{f^d}\right|. \end{aligned}$$

□

Corollary 2. *If $f : X \to X$ and the set F_{f^n} is finite, then*

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) \cdot \left|F_{f^d}\right| \equiv 0 (\text{mod } n). \tag{3}$$

Remark 2. Using a similar calculation we can prove that for an arbitrary sequence $(x_n)_{n \geq 1}$ the relations

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot x_d \equiv 0 (\text{mod } n), \quad n \geq 1 \tag{4}$$

and

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) \cdot x_d \equiv 0 (\text{mod } n), \quad n \geq 1 \tag{5}$$

are equivalent.

Example 1. For the function $f : [0,1] \to [0,1]$, $f(x) = \{ax\}$ ($a \in \mathbb{N}^*$, $a \geq 2$ and $\{u\}$ denotes the fractional part of u) we have $|F_{f^n}| = a^n - 1$, for $n \geq 1$, hence Corollary 1 and Corollary 2 imply

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) (a^d - 1) \equiv 0 (\text{mod } n), \quad \forall n \geq 1 \tag{6}$$

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) (a^d - 1) \equiv 0 (\text{mod } n), \quad \forall n \geq 1. \tag{7}$$

Using

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) = \begin{cases} 1, & n = 1 \\ 0, & n \geq 2 \end{cases} \quad \text{and} \quad \sum_{d|n} \varphi\left(\frac{n}{d}\right) = n$$

we obtain

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) (a^d - 1) \equiv 0 (\text{mod } n), \quad \forall n \geq 1 \tag{8}$$

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) (a^d - 1) \equiv 0 (\text{mod } n), \quad \forall n \geq 1. \tag{9}$$

Both of these congruencies can be viewed as generalizations of the little Fermat theorem.

Example 2. For $f : [0,1] \to [0,1]$ defined by

$$f(x) = \begin{cases} x + \frac{1}{2}, & \text{if } x < \frac{1}{2} \\ 2 - 2x, & \text{if } x \geq \frac{1}{2} \end{cases}$$

we have $|F_{f^n}| = L_n$, $\forall n \geq 1$, where $(L_n)_{n \geq 1}$ are the Lucas numbers (see [4]), so

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot L_d \equiv 0 (\text{mod } n), \quad \forall n \geq 1 \tag{10}$$

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) \cdot L_d \equiv 0 (\text{mod } n), \quad \forall n \geq 1. \tag{11}$$

Example 3. The sequence

$$s_1 = 2,\ s_2 = 8,\ \ s_{n+2} = 2s_{n+1} + 2s_n,\ \forall n \geq 1$$

satisfies the following congruencies

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot s_d \equiv 0 (\text{mod } n), \quad \forall n \geq 1 \tag{12}$$

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) \cdot s_d \equiv 0 (\text{mod } n), \quad \forall n \geq 1. \tag{13}$$

This sequence corresponds to the function $f : [0,1] \to [0,1]$,

$$f(x) = \begin{cases} 3x, & x \in [0, 1/3) \\ 2 - 3x, & x \in [1/3, 2/3) \\ 2x - 4/3, & x \in [2/3, 1] \end{cases}$$

in the sense that $s_n = |F_{f^n}|$, $\forall n \geq 1$.

Remark 3. Relation (9) appears in [6] as Theorem 1. Examples 2 and 3 show that this congruence can be extended to linear recurrent sequences. More precisely if $p \in \mathbb{N}^*$, $\alpha_0, \alpha_1, \ldots, \alpha_{p-1} \in \mathbb{N}$, then there exists $x_0, x_1, \ldots, x_{p-1} \in \mathbb{N}$ such that the sequence $x_{n+p} = \sum_{j=0}^{p-1} \alpha_j x_{n+j}$, $n \geq 0$ satisfies (4) and (5).

3 An alternative proof for the generalization of Wilson's theorem

Denote the number of oriented Hamiltonian cycles over the vertices of a regular n-gon which are invariant under the rotation of angle $2d\pi/n$ by $|F_{f^d}|$, the number of oriented Hamiltonian cycles whose period (under rotations) is d by $|P_f(d)|$ and the number of nonequivalent (by rotation) oriented Hamiltonian cycles by $|HC_n|$.

Theorem 3. *For every $n \geq 1$ and $d|n$*

a) $|F_{f^d}| = \varphi\left(\frac{n}{d}\right) \cdot \left(\frac{n}{d}\right)^{d-1} \cdot (d-1)!$;

b) $|P_f(d)| = \sum_{d|n} \mu\left(\frac{n}{d}\right) \varphi\left(\frac{n}{d}\right) \cdot \left(\frac{n}{d}\right)^{d-1} \cdot (d-1)!$;

c) $|HC_n| = \frac{1}{n} \cdot \sum_{d|n} \varphi^2\left(\frac{n}{d}\right) \cdot \left(\frac{n}{d}\right)^{d-1} \cdot (d-1)!$.

Remark 4. The relation c) appears in [6] as Theorem 2.

Proof. Label the vertices of the regular n-gon by $0, 1, 2, \ldots, n-1$. First we claim that if $d > 1$, $d|n$ and K is an oriented Hamiltonian cycle, which is invariant under the rotation of angle $d \cdot \frac{2\pi}{n}$, then the difference of two labels from the endpoints of any segment belonging to K is not a multiple of d. Suppose the contrary. By rotating this cycle around the center of the polygon we can assume that the labels in the vertices are 0 and $\nu \cdot d$ ($\nu \in \mathbb{N}$). Consider the remainder modulo n of each number in the following pairs:

$$(0, \nu \cdot d), (d, (\nu+1) \cdot d), \ldots, (n - \nu d, 0)$$

Each segment whose endpoints are labeled with these remainder-pairs are segments in K. But $d|n$, so these segments form a closed cycle which avoids the vertex 1. In

the same manner we prove that if $d = 1$ and the endpoint of the segment starting from 0 is ν, then the greatest common divisor of ν and n is 1. If K is invariant under the rotation of angle $\frac{2\pi}{n}$, then the segments $(\nu, 2\nu), ..., (k\nu, (k+1)\nu)$ are in K. But if $\gcd(n, \nu) > 1$, then these segments form a closed cycle which avoids the vertex 1. It is sufficient to construct the first d vertices of the cycle, because from the invariance we can obtain the rest of the cycle by rotations (each segment e determines other $n/d-1$ segments, which are obtained from e by rotations of $2\pi d/n, 4\pi d/n, \ldots, 2(n-d)\pi/n$). Hence the endpoint of the segment starting from 0 can be chosen in $\left(n - \frac{n}{d}\right)$ ways, the next point can be chosen in $\left(n - \frac{2 \cdot n}{d}\right)$ ways and so on. This can be continued to obtain $\frac{n}{d}$ congruent pieces. The starting point of these pieces are labeled with $0, d, 2d, \ldots, n-d$, so by identifying the pieces with their starting points we obtain a regular n/d-gon. This implies that the endpoint of the piece starting from 0 can be joined with the starting point of $\varphi\left(\frac{n}{d}\right)$ other pieces (otherwise we do not obtain a single cycle passing through all the vertices), so we obtain $\left(\frac{n}{d}\right)^{d-1} \cdot (d-1)! \cdot \varphi\left(\frac{n}{d}\right)$ cycles which are invariant under the rotation of $\frac{2d\pi}{n}$. The proof is completed using Theorems 1 and 2. □

Remark 5. For $n = 6$ we illustrated the equivalence classes of the directed Hamiltonian cycles in figure 1 by representing one cycle from each class. Here d denotes the period of the cycles, so there exists 2 classes with period $1, 2$, and 3 and 18 classes with period 6. This gives $F_1 = 2, F_2 = 2 + 2 \cdot 2 = 6, F_3 = 2 + 2 \cdot 3 = 8$ and $F_6 = 2 + 2 \cdot 2 + 2 \cdot 3 + 18 \cdot 6 = 120$, and these results are those obtained from the formula $\left(\frac{n}{d}\right)^{d-1} \cdot (d-1)! \cdot \varphi\left(\frac{n}{d}\right)$ for $n = 6$ and $d \in \{1, 2, 3, 6\}$.

Corollary 3. *For $n \geq 1$ we have*

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \varphi\left(\frac{n}{d}\right) \cdot \left(\frac{n}{d}\right)^{d-1} \cdot (d-1)! \equiv 0 (\text{mod } n) \tag{14}$$

$$\sum_{d|n} \varphi^2\left(\frac{n}{d}\right) \cdot \left(\frac{n}{d}\right)^{d-1} \cdot (d-1)! \equiv 0 (\text{mod } n). \tag{15}$$

4 Concluding remarks

If $n = p$ is a prime number, from (14),(15) we obtain

$$|HC_p| = \frac{(p-1)! + (p-1)^2}{p}, \text{ and } |P_f(p)| = (p-1)! - (p-1),$$

so both of the relations (14),(15) can be viewed as generalizations of Wilson's theorem.

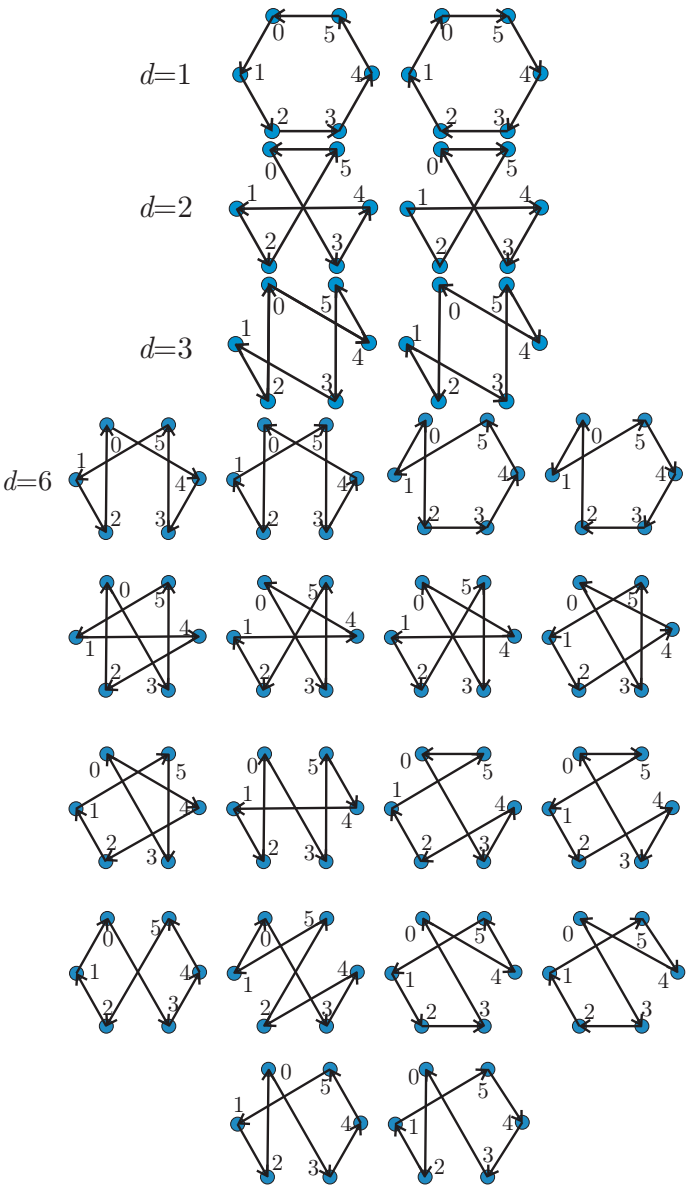

Figure 1: Oriented Hamiltonian cycles on the vertices of a regular hexagon; d represents the period of the corresponding cycles

In [6] relation (15) is proved by counting the orbits of the action of $\mathbb{Z}_n$ over the set of all cycles of length n in the symmetric group S_n. Every cycle $\gamma \in S_n$ of length n can be identified with an oriented cycle over the vertices of a regular n-gon (there is an oriented edge from i to j exactly when $\gamma(i) = j$). Hence the action of the element $\hat{k} \in \mathbb{Z}_n$ over a cycle $\gamma \in S_n$ can be identified with the rotation of angle $2k\pi/n$ of the cycle determined by γ. This connection shows that we counted the same orbits as the author of [6].

Theorem 2 can be useful in many other problems. The idea appears also in [1], but only in the special case of necklace counting (which is equivalent to Example 1).

References

[1] E.A. Bender and J.R. Goldman, On the applications of Möbius inversion formula in combinatorial analysis, *Amer. Math. Monthly* 82 (1975), 789–803.

[2] A.T. Benjamin and J.J. Quinn, *Proofs That Really Count, The Art of Combinatorial Proofs*, Mathematical Association of America, Providence, 2003.

[3] D.M. Burton, *Elementary number theory*, Allyn and Bacon Inc., 1980.

[4] J. Bobok and L. Snoha, Peridic points and Little Fermat Theorem, *Nieuw Archiev voor Wiskunder* 10 (1992) No. 1–2, 33–35.

[5] T.J. Evans and B.V. Holt, Deriving Divisibility Theorems With Burnside's Theorem, *Integers: Electr. J. Combin. Number Theory* (2005), 5(1).

[6] T.J. Evans, On some generalizations of Fermat's, Lucas's and Wilson's theorems, *Ars Combin.* 79 (2006), 189–194.

[7] P. Hajnal, *Elementary combinatorial problems* (in Hungarian), Polygon, Szeged, 2005.

[8] K. Härtig and J. Surányi, Combinatorial and geometrical investigations in elementary number theory, *Period. Math. Hung.* 6 (1975), 235–240.

[9] L. Levine, Fermat's little theorem: A proof by function iteration, *Math. Magazine* 72 (1999), No. 4, 308–309.

[10] R. Merris, *Combinatorics*, Wiley-Interscience, 2003.

[11] K. Rosen (ed.), *Handbook of discrete and combinatorial mathematics*, CRC Press, 1999.

(Received 2 Oct 2010; revised 24 Nov 2010)