Bull. Math. Soc. Sci. Math. Roumanie
Tome 56(104) No. 3, 2013, 331–334

The Y factor

by
Marian Deaconescu and Gary Walls

Dedicated to Professors Toma Albu and Constantin Năstăsescu on the occasion of their 70th birthdays

Abstract

Combinatorial methods are applied to the holomorph of a cyclic group in order to derive, among other things, a statement that sheds some light on the well-known "totient" conjecture of D.H. Lehmer.

Key Words: Cyclic group, holomorph, automorphisms, orbits, Lehmer numbers.
2010 Mathematics Subject Classification: Primary 20D60;
Secondary 11A25, 11N80.

This note was inspired by a well-known conjecture of D. H. Lehmer [4]: an integer $n \geq 2$ is a prime if and only if $\varphi(n)$ divides $n-1$. We are not solving this conjecture here, but we use it as a good excuse to make some remarks on the holomorphs of cyclic groups of very special order. The precise aim is to show that these holomorphs could be very interesting objects from a combinatorial point of view. Miller [5] wrote a paper on holomorphs of cyclic groups about one hundred and ten years ago and, strolling on old trails, could be very rewarding indeed.

The unexplained notation is mostly standard. G will be a finite group of order $n \geq 3$, so its automorphism group $A = Aut(G)$ will always contain a nontrivial automorphism (i.e., distinct from the identity map id_G). We will work in the holomorph $H = Hol(G)$ of G; this can be viewed as the semidirect product $GA = AG$, with the base group G normal in H, with $C_A(G) = 1$ and $G \cap A = 1$.

If $1 \in S \subseteq H$, we will write $S^\star$ instead of $S \setminus \{1\}$. We write H as the union of three mutually disjoint subsets: $G^\star$, $X = \bigcup_{g \in G} A^g$ and $Y = H \setminus (G^\star \cup X)$.

We let both G and A act by conjugation on H and we observe that all of the three subsets mentioned above are G-invariant and A-invariant. Hence they are also H-invariant (i.e., unions of conjugacy classes in H).

Whenever a group Y acts on a group X, we will denote by x^Y the orbit of $x \in X$ under the action of Y. Also, we will denote by $t_Y(X)$ the number of orbits of Y in X. For example, for $a \in A$, we have that $a^G = \{a^g \mid g \in G\}$. It is well-known that $|a^G| = |G : C_G(a)|$, where $C_G(a)$ denotes the subgroup of all fixed-points of a in G. Since $G \cap A = 1$, it is easy to see

that distinct elements of A have distinct G-orbits. This shows at once two things: first, that G acts with exactly $|A|$ orbits on the subset X and that $|X| = \sum_{a \in A} |G : C_G(a)|$. And, since by definition $|Y| = |G||A| - |G| + 1 - |X|$, we obtain that

$$|Y| = \sum_{a \in A^\star} (|G| - |G : C_G(a)|)$$

.

These considerations are not really new, for the set $X^\star$ was considered a long time ago in connection with the so-called Frobenius groups. We are dealing with the set X here for number -theoretical reasons that will become clearer below.

Something similar works for computing the number of G-orbits contained in Y.

Let $t_A(G)$ be the number of orbits of A in its natural action on G and let $k(G) = t_G(G)$ denote the number of G-orbits in G (these are nothing else but the conjugacy classes of G). As done in [3], an application of the Cauchy-Frobenius Lemma shows that G has exactly $t_A(G)|A|$ orbits in H. Thus G has in Y exactly $t_A(G)|A| - k(G) + 1 - |A|$ orbits and hence Y is empty precisely when G acts with zero orbits on Y, i.e., when $|A|(t_A(G) - 1) = k(G) - 1$.

But Y is empty precisely when $C_G(a) = 1$ for all $a \in A^\star$. And this happens precisely when $|G| = p$ is a prime. Indeed, it must be clear that G is abelian, for the nontrivial inner automorphisms don't act fixed-point-freely on G. It is also clear, via the Frobenius-Stickelberger theorem, that G must be a cyclic p-group. And then, one derives that $|G| = p$. Conversely, when $|G| = p \geq 3$, then $|A| = p - 1$, $k(G) = |G| = p$ and $t_A(G) = 2$. And, finally, the exceptional case when $|G| = 2$ being trivial, we have proved

Proposition 1. *Let G be a finite group with $|G| \geq 2$. Then $|G|$ is a prime if and only if $|A|(t_A(G) - 1) = k(G) - 1$.*

If one wants to determine the number of A-orbits in Y in this general setting, the task becomes complicated. This is due to the fact that the numbers of orbits of A in H and in X are harder to get in general.

However, this can be done provided that G is a group of a very special order. If $\phi := \varphi(n)$, call $n \geq 2$ a *Lehmer number* if the equality $n = a\phi + 1$ holds for some positive integer a. Of course, every prime is a Lehmer number (this happens precisely when $a = 1$) and Lehmer's conjecture asserts that there are no composite such numbers.

From now on, if nothing else is specified, G will be a group having $n \geq 3$ elements, where $n = a\phi + 1$ is a Lehmer number. Then $(n, \phi) = 1$ and it is immediate that n must be odd and square-free, with a number, say, of $s \geq 1$ distinct prime factors. It is a well-known exercise that G must be a cyclic group, so A is abelian in this case and we have that $|A| = \phi$ and that $t_A(G) = 2^s$ is the number of divisors of $|G| = n$. Also , if $a \in A$, then it is well-known that $G = C_G(a) \times K_G(a)$, where $K_G(a) = \{[g, a] \mid g \in G\}$. Note that in general the set $K_G(a)$ is not necessarily a subgroup of G, but in our case it is, for G is abelian.

If d is any divisor of n, write $\psi(d) := \prod_{p|d}(p - 2)$. Here the product is taken over all primes dividing d and, by customary convention, $\psi(1) = 1$. It was shown in [1] that there exist exactly $\psi(\frac{n}{d})$ automorphisms $a \in A$ such that $|C_G(a)| = d$.

We claim now that when $|G| = n$ is a Lehmer number, then $|X| = \phi^2$. Indeed, $|X| = \sum_{a \in A} |G : C_G(a)| = \sum_{d|n} \frac{n}{d}\psi(\frac{n}{d}) = \sum_{d|n} d\psi(d) = \prod_{p|n}(1 + p(p - 2)) = \phi^2$.

It is now easy to determine the size of Y, for $|Y| = |G||A| - |G| + 1 - |X| = n\phi - n + 1 - \phi^2 = n\phi - a\phi - \phi^2 = \phi(n - a - \phi) = (\phi - 1)(n - \phi - 1) = \phi(\phi - 1)(a - 1)$.

It is also easy to determine the number of G-orbits in Y. Note that in our case ($|G| = n$ is square-free), $t_A(G)$ is the number of divisors of n, which is 2^s, where s is the number of prime factors of n. Thus, according to our general setting above, G has exactly $2^s\phi - n + 1 - \phi$ orbits in Y (this is because G being abelian we have $k(G) = |G|$). And so, since $n = a\phi + 1$, we get that G has exactly $\phi(2^s - a - 1)$ orbits on Y.

The problem of the number of A-orbits in X is a bit more complicated.

Observe first that, for $a \in A$ fixed, the G-orbit a^G is A-invariant. Indeed, $a^G = \{a^g \mid g \in G\} = aK_G(a)$ and so, if $b \in A$, we have that $(a^G)^b = (aK_G(a))^b = a^b(K_G(a))^b = aK_G(a) = a^G$. This is because G is cyclic, so A is abelian and also $K_G(a)$ is characteristic in G (or, if the reader prefers so, normal in H). The number of orbits of A on a^G is thus exactly the number of orbits of A on the subgroup $K_G(a)$. And this number is equal to the number of divisors of $|K_G(a)|$.

Therefore, the total number of A-orbits in X is equal to a sum of powers of 2, each one appearing , for some divisor $d = |C_G(a)|$ of n exactly $\psi(\frac{n}{d})$ times. That number is then equal to $\sum_{d|n} 2^{s_d}\psi(\frac{n}{d})$, where s_d denotes here the number of divisors of $\frac{n}{d} = |G : C_G(a)| = |K_G(a)|$, so the sum in discussion is actually equal to $\prod_{p|n}(1 + 2(p - 2)) = \prod_{p|n}(2p - 3)$.

Finally, in order to compute the number of A-orbits in Y, we only need the number of A-orbits in H. This was shown in [3] to be (because A is abelian) equal to $t_A(G)|A|$. And so, since A acts with $t_A(G) - 1$ orbits on $G^\star$, the number of A orbits on Y is equal to

$$t_A(G)|A| - t_A(G) + 1 - \prod_{p|n}(2p - 3) = 2^s\phi - 2^s + 1 - \prod_{p|n}(2p - 3)$$

.

From what was said above, we retain only this rather surprising result - the exceptional case when $|G| = 2$ is, again, trivial.

Proposition 2. *Let G be a group of order $n \geq 2$. Then n is a Lehmer number if and only if $|A|(|A| - 1)$ divides $|Y|$. Therefore, n is a counterexample to Lehmer's conjecture if and only if $|Y|$ is a nonzero multiple of $\phi(\phi - 1)$.*

Some comments are in order here, the first being that the equality $|X| = \phi^2$ holds whenever G is cyclic of square-free order (for only this is what was used in proof). It fails to hold when G is cyclic of order four. For in that case, G has just two automorphisms, one fixing G and one fixing the subgroup of order 2 of G, yielding $|X| = 3$.

The second comment is that it was shown in [2] by elementary calculations that if n is a Lehmer number and if also $n \mid \phi^2 - 1$, then n must be a prime. We can now give a more conceptual proof to this observation: since n is a Lehmer number, it follows that ϕ divides $|Y|$. Since n divides $\phi^2 - 1$, it follows that n divides $|Y|$. And, since $(n, \phi) = 1$, it follows that $n\phi = |G||A| = |H|$ divides $|Y|$. This could only happen when $|Y| = 0$, i.e. when n is a prime.

Finally, since we did not discuss that problem here, it remains the interesting question of finding the number of orbits of H in its conjugation action on both X and Y in the very special case when $|G|$ is a Lehmer number.

References

[1] Marian Deaconescu and Hang K. Du, *Counting similar automorphisms of finite cyclic groups*, Math. Jap. **46** (1997) 345–348.

[2] Marian Deaconescu, *On the equation* $m - 1 = a\varphi(m)$, Itegers (2006), paper A06, 6pp.

[3] Marian Deaconescu and Gary Walls, *On groups acting on groups*, submitted.

[4] D.H. Lehmer, *On Euler's totient function*, Bull. Am. Math. Soc. **38** (1932) 745–751.

[5] G.A. Miller, *On the holomorph of a cyclic group*, Trans. Am. Math. Soc. **4** (1903) 153–160.

Received: 1.03.2013,
Accepted: 21.03.2013.

Department of Mathematics,Kuwait University, P.O. Box 5969, Safat 13060, Kuwait
E-mail: mdeaconescu@yahoo.com

Department of Mathematics, Southeastern Louisiana University, Box 10687, Hammond, LA 70402, U.S.A.
E-mail:gary.walls@selu.edu