Classroom

In this section of *Resonance*, we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

Anjana Khurana and Dinesh Khurana
Department of Mathematics
Panjab University
Chandigarh 160 014, India.
Email: an14in@yahoo.com
dkhurana@pu.ac.in

Conjugacy Classes in Alternating Groups

In undergraduate courses in mathematics, one of the first groups one comes across is the set of all permutations of a finite set. Although such a description makes it seem like an easy object to study, one soon learns that it is not so, as every finite group sits in it. The set of all even permutations (that is, those obtained after an even number of exchanges) of n objects, forms a subgroup, the so-called alternating group, denoted by A_n. The simple groups are the basic building blocks and the smallest such group in size is A_5 which has order 60. One learns in a first course that A_n is simple for any $n \geq 5$. Since a normal subgroup is a union of certain conjugacy classes of the group, it follows that no proper union of conjugacy classes in A_n ($n \geq 5$) forms a subgroup.

For instance, there are five conjugacy classes in A_5 and the orders of non-trivial ones are 12, 12, 15 and 20. When m runs through proper sums of these orders, then $1+m$ runs through the numbers 13, 16, 21, 25, 28, 33, 36, 40, 45 and 48. None of these divide the order 60 of A_5. Therefore, A_5 is simple. A similar argument works for A_6 by finding the orders of its conjugacy classes. *It is useful to keep in mind that, in S_n, conjugacy classes are determined by the manner in which permutations break into disjoint cycles.*

Keywords
Surfaces of revolution, vector algebra, parametric equation, cardioid, Möbius strip.

For the past several years R N Gupta has been asking if one can prove the simplicity of A_n ($n \geq 5$) this way. In other words does $1+m$ ever divide $n!/2$, where m is any proper sum of orders of non-trivial conjugacy classes in A_n with $n > 4$. It turns out surprisingly that the answer to Gupta's question is in the negative and $n = 68$ seems to be the smallest counterexample.

The order of A_n and the orders of its conjugacy classes increase too rapidly with n, to handle manually. For instance, the order of A_{12} is 239500800 and the order of the conjugacy class of 11-cycles is 21772800. The order of the conjugacy class of three cycles in A_n, which is given by $\frac{n(n-1)(n-2)}{3}$, is usually the smallest such order; for example, it is 440 in A_{12} (the tables of conjugacy classes of A_{11} and A_{12} provided by Gupta were useful). Thus we start with the simplest case where m is the order of the conjugacy class of 3-cycles i.e., $m = \frac{n(n-1)(n-2)}{3}$. Now we have to check whether for some natural number n, $(1 + \frac{n(n-1)(n-2)}{3})|n!/2$, where $a|b$ means that a divides b. But $n!/2$ soon becomes so large that even ordinary computers fail to check divisibility of $n!/2$ by $1 + \frac{n(n-1)(n-2)}{3}$ directly.

We write $a^n||b$ to mean that n is the highest power of a dividing b. For $n > 4$, a prime p divides $n!/2$ if and only if $p \leq n$. Then, we have

LEMMA. $(1 + \frac{n(n-1)(n-2)}{3})|n!/2$ *if and only if*

(i)For any prime p, $p|1 + \frac{n(n-1)(n-2)}{3} \Rightarrow p \leq n$;

(ii) For any prime p, $p^l||1 + \frac{n(n-1)(n-2)}{3}$ *and* $p^t||n!/2 \Rightarrow l \leq t$.

With the help of the following computer program in FORTRAN, we check that from 5 to 250 only $n = 12, 14, 68, 149, 179, 247$ satisfy the condition (i) of the Lemma above. This program picks n from 5 to 250 and checks whether $k = 1 + \frac{n(n-1)(n-2)}{3}$ is divisible by a prime

p such that $p \leq n$. If $p|k$ then k is replaced by $k = k/p$. Now the program checks whether $p|k/p$ and so on and then goes to the rest of primes. If on checking for all primes $p \leq n$, k becomes equal to 1, then n satisfies the condition (i) of the Lemma.

```
      integer m, n, k, l
      do 10 n=5,250,1
      k = (n * (n - 1) * (n - 2)/3) + 1
60    if(mod(k, 2).eq.0)then
      k = k/2
      goto 60
      endif
      do 20 j = 2, n, 1
      do 30 i = 2, j - 1, 1
      b = mod(j, i)
      if(b.eq.0)then
      goto 20
      endif
      if(b.ne.0)then
      if(i.eq.j - 1)then
      goto 50
      endif
      endif
30    continue
50    a = mod(k, j)
      if(a.eq.0)then
      k = k/j
      goto 50
      else
      goto 20
      endif
20    continue
      if(k.eq.1)then
      write(*, *)n
      endif
10    continue
      stop
      end
```

Now to see which of the n's among $12, 14, 68, 149, 179, 247$ satisfy the condition (ii) of the Lemma above, we write the prime factorization of $k = 1 + \frac{n(n-1)(n-2)}{3}$ for each of these n's as follows.

For $n = 12$, $1 + \frac{n(n-1)(n-2)}{3} = 441 = 3^2.7^2$;

For $n = 14$, $1 + \frac{n(n-1)(n-2)}{3} = 729 = 3^6$;

For $n = 68$, $1 + \frac{n(n-1)(n-2)}{3} = 100233 = 3^2.7.37.43$;

For $n = 149$, $1 + \frac{n(n-1)(n-2)}{3} = 1080549 = 3^2.19.71.89$;

For $n = 179$, $1 + \frac{n(n-1)(n-2)}{3} = 1879859 = 23.37.47^2$;

For $n = 247$, $1 + \frac{n(n-1)(n-2)}{3} = 4962231 = 3^2.53.101.103$.

As 7 appears only once in the prime factorization of $12!/2$ and 3 appears in $5th$ power in the prime factorization of $14!/2$, $n = 12$ and $n = 14$ do not satisfy the condition (ii) of the Lemma. So $n = 68$ is the first natural number such that $(1 + \frac{n(n-1)(n-2)}{3}) | n!/2$. This answers Gupta's question in the negative. Note that $(1 + \frac{n(n-1)(n-2)}{3}) | n!/2$ for $n = 149, 179, 247$ also.

Two Interesting Questions

It is interesting to note that if m is the order of conjugacy class of (1,2)(3,4) in A_n, i.e., $m = \frac{n(n-1)(n-2)(n-3)}{8}$, then $1 + m$ does not divide $n!/2$ for all $n \leq 200$. This makes one ask the following:

Question 1.

Does $(1 + m) | n!/2$, $n > 4$, *where* m *is a proper sum of the sizes of conjugacy classes, other than the conjugacy class of* 3*-cycles, of* A_n*?*

As A_n, $n > 4$, is generated by 3-cycles, a negative answer to the above question will still prove the simplicity of A_n, $n > 4$.

In another direction, let us look at the subset $S = \{x \in G : x^d = 1\}$ in any finite group G, where d is a divisor of the order of G. Now, S is a union of certain conjugacy classes of G including the identity conjugacy class. From a theorem of Frobenius (see [1] or [2]) it follows that the order of S is dt for some natural number t. Rust [3], proving a conjecture of Frobenius for A_n ($n \geq 5$), showed that $t > 1$. This begs the following question:

Question 2.

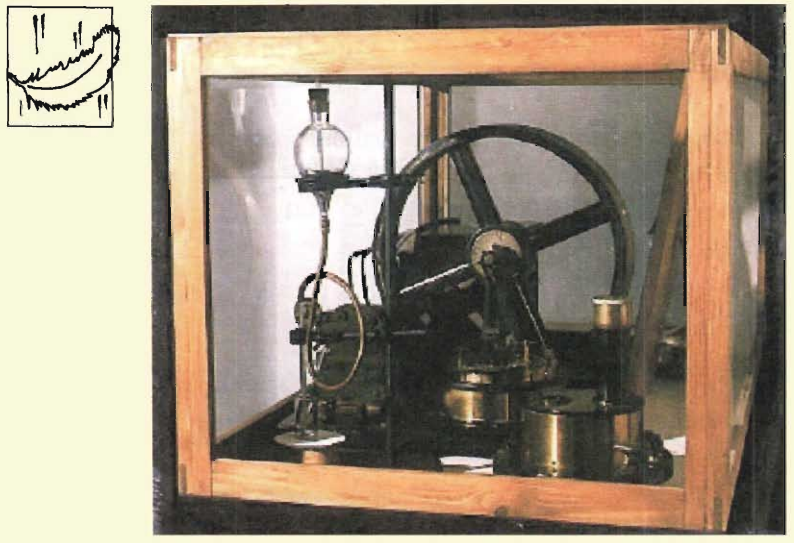
Let d be a divisor of $n!/2$ ($n \geq 5$) and $S = \{x \in A_n : x^d = 1\}$. If $S \neq A_n$, then does order of S divide $n!/2$?

Suggested Reading

[1] R Brauer, On a theorem of Frobenius, *Amer. Math. Monthly*, Vol.76, pp. 12-15, 1969.

[2] Dinesh Khurana and Anjana Khurana, *On a theorem of Frobenius and its applications*, preprint.

[3] J Rust, *On a Conjucture of Frobenius*, PhD Thesis, Univ of Chicago, 1966.



Picture of the first polarograph designed by J Heyrovský and M Shikata (1924).

Source: http://chem.ch.huji.ac.il/~eugeniik/history/heyrovsky.htm