93.24 Vandermonde for cyclicity

While teaching a course in group theory to undergraduates, many of us would have faced the following familiar dilemma. Although cyclic groups can be discussed quite early, and one can introduce the group Z_p^* with the multiplication modulo p for a prime number p as an example, one defers the proof until the introduction of fields. Of course, this example itself belongs to number theory and is probably discussed in a course on that subject. It may be worthwhile to have an alternative method of proof which could be given while discussing group theory itself. Here is a proof which assumes a bit about matrices. Two facts about matrices which one may prove beforehand are:

Fact I :

For any square matrix A, $\mathrm{adj}(A).A = (\det A)I$.

Fact II :

For numbers $a_1, \ldots, a_n$, the Vandermonde matrix $\begin{pmatrix} 1 & a_0 & a_0^2 & \ldots & a_0^n \\ 1 & a_1 & a_1^2 & \ldots & a_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^n \end{pmatrix}$

has determinant equal to $\prod_{n \geqslant i > j \geqslant 0} (a_i - a_j)$.

This can, of course, be proved by induction.

Lemma

Let p be a prime and let $1 \leqslant n < p$. Then there are at most n elements of Z_p^* which satisfy $a^n = 1$ in this group.

Proof:

Suppose not. Let $a_0, a_1, \ldots, a_n$ be distinct elements each satisfying $a_i^n = 1$ in Z_p^*. Thus, $a_0, a_1, \ldots, a_n$ can be viewed as positive integers (all $< p$) such that p divides each $a_i^n - 1$. Let b_i be integers with $pb_i = a_i^n - 1$ for $i = 0, 1, 2, \ldots, n$. Thus, we have the matrix equation

$$\begin{pmatrix} 1 & a_0 & a_0^2 & \ldots & a_0^n \\ 1 & a_1 & a_1^2 & \ldots & a_1^n \\ 1 & a_2 & a_2^2 & \ldots & a_2^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^n \end{pmatrix} \begin{pmatrix} -1 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} pb_0 \\ pb_1 \\ pb_2 \\ \vdots \\ pb_n \end{pmatrix}.$$

Multiplying on the left by $\mathrm{adj}(A)$, we have

$$\begin{pmatrix} -\det A \\ 0 \\ \vdots \\ 0 \\ \det A \end{pmatrix} = \operatorname{adj}(A) \begin{pmatrix} pb_0 \\ pb_1 \\ pb_2 \\ \vdots \\ pb_n \end{pmatrix}.$$

As $\operatorname{adj}(A)$ has entries from the integers, the right-hand side above is of the form $\begin{pmatrix} pc_0 \\ pc_1 \\ \vdots \\ pc_n \end{pmatrix}$ where $c_0, c_1, \dots, c_n$ are integers. Thus, $pc_1 = \det A = \prod_{i>j}(a_i - a_j)$, which is impossible as all the a_i are distinct and less than p.

Of course, the above analysis clearly proves the following more general result:

Theorem

Let p be a prime. Let $1 \leqslant n < p$ and $f(x) = c_0 + c_1x + \dots + c_nx^n$ be any polynomial with integer coefficients. Then there are at most n solutions of $f(x) \equiv 0 \bmod p$ unless $c_i \equiv 0 \bmod p$ for all i.

The deduction of cyclicity of Z_p^* from the lemma is quite well-known. Textbooks in algebra, for example [1], use the fact that finite abelian groups are direct products of cyclic groups. But, one may prove it before discussing finite abelian groups. The following argument is also well known :

Let G be a possibly nonabelian group in which, for every r, the number of elements satisfying $x^r = e$ is at most r. Let G have order n and $d \mid n$.

Write $N(d)$ for the size of the set $\{g \in G : O(g) = d\}$.

If $N(d) \neq 0$, look at some element g with $O(g) = d$. As $e, g, g^2, \dots, g^{d-1}$ are distinct and are solutions of $x^d = e$, these are *all* the solutions of the equation $x^d = e$. As elements of order d in G are among these and are $\phi(d)$ in number, we have that $N(d) = \phi(d)$ if $N(d) \neq 0$. As every element of G has some order d dividing n, we have $n = \sum_{d \mid n} N(d)$. Since $n = \sum_{d \mid n} \phi(d) \geqslant \sum_{d \mid n} N(d) = n$, we must have the equality $N(d) = \phi(d)$ for all $d \mid n$. In particular, $N(n) = \phi(n) \neq 0$.

Acknowledgements

It is a pleasure to thank a referee who has made interesting and constructive comments. In particular, it resulted in my changing the initial premise which was to view this proof as more natural, to the present one

which is to merely view this as an alternative path to the result. Regarding another suggestion of the referee, I have preferred to keep the lemma over integers itself as I feel it is perhaps transparent.

Reference

1. I. N. Herstein, PLEASE SUPPLY TITLE AND OTHER DETAILS

B. SURY

Statistics & Mathematics Unit, Indian Statistical Institute,

8th Mile Mysore Road, Bangalore 560 059, India

e-mail: *sury@isibang.ac.in*