**Group theory lends a hand to number theory**

**B.Sury**

Many congruences in elementary number theory can be rephrased in the language of group theory. Apart from being interesting in its own right, the group-theoretic rephrasing often gives a more conceptual proof of a number-theoretic result such as Fermat's little theorem. Consider the group $\mathbf{Z}_n^*$ of integers less than $n$ and co-prime to $n$ under multiplication modulo $n$. The classical Wilson's congruence $(p-1)! \equiv -1 \bmod p$ for a prime $p$ can be viewed as the assertion $\prod_{a\in\mathbf{Z}_p^*} a = p-1$. Each element cancels out with its inverse and we are left with the product of all those elements which are their own inverses. As $p$ is prime, $p|(a^2-1)$ has the two solutions $a = 1, p-1$; hence, the product of all the elements of this group is $p-1$, which gives the Wilson congruence. The immediate question which arises after looking at the above proof is what happens for a non-prime $n$ when we look at the product $\prod_{a\in\mathbf{Z}_n^*} a$. The interesting result which emerges is embodied in the following signature lemma - so christened because it gives us the values $\pm 1$ depending on whether primitive roots mod $n$ exist or not.

**Signature lemma.**
*If $s(n)$ denotes the product of all the elements of $\mathbf{Z}_n^*$, we have $s(n) = -1$ if $n = 2, 4, p^k$, or $2p^k$ for some odd prime $p$ and some $k \geq 1$. If $n$ is none of these, then $s(n) = 1$. In other words, by the well-known characterization of numbers which admit primitive roots, we have $s(n) = \mp 1$ according as to whether $\mathbf{Z}_n^*$ is cyclic or not.*

**Proof.**
If $\mathbf{Z}_n^*$ is cyclic, then for any generator $a$, we have

$$s(n) = \prod_{i=1}^{\phi(n)} a^i = a^{\sum_i i} = a^{(\phi(n)+1)\phi(n)/2} = a^{\phi(n)/2}.$$

In a cyclic group of even order, there is a unique subgroup of order 2 and so $-1$ is the only element of order 2 in $\mathbf{Z}_n^*$. But, since $s(n)$ above clearly has order 2, it follows that $s(n) = -1$ when $\mathbf{Z}_n^*$ is cyclic. Note that this also includes the trivial group $\mathbf{Z}_2^*$ as $1 = -1$ in it.
As we are in an abelian group, in the product $s(n)$, all elements cancel with their inverses except for those elements which are their own inverses. In other words, $s(n)$ is the product of all $a \in \mathbf{Z}_n^*$ which satisfy $a^2 = 1$.

For a prime $n$, this is Wilson's theorem.
We suppose $n$ is arbitrary and $> 2$. Now, each such $a$ in $\mathbf{Z}_n^*$ has a unique $b$ for which $ab = -1$. Clearly, $b^2 = 1$ as well. Moreover, as $n \neq 2$, $b \neq a$.
Hence if $N(n)$ denotes the number of elements $a$ such that $a^2 = 1$, then we have $s(n) = (-1)^{N(n)/2}$. Now, clearly $N(n)$ is the order of $\mathbf{Z}_n^*/(\mathbf{Z}_n^*)^2$ as it is the order of the kernel of the squaring map on $\mathbf{Z}_n^*$. But, from the Chinese remainder theorem, note that under the isomorphism of $\mathbf{Z}_n^*$ with the product of $\mathbf{Z}^*_{p_i^{k_i}}$ where $n = \prod_i p_i^{k_i}$, the squares in $\mathbf{Z}_n^*$ map onto the squares in each component. Hence $N(n)$ is a multiplicative function. Note that $N(n)$ is even for all $n > 2$ since in a group of even order, the number of elements of exponent 2 is even. Now, we consider an arbitrary $n > 1$ and the corresponding $N(n)$. As noted above, if $n = \prod_{i=1}^r p_i^{k_i}$, then $N(n) = \prod_{i=1}^r N(p_i^{k_i})$. Thus, if $r > 1$, then $N(n) \equiv 0 \bmod 4$ unless $n = 2p^k$ for some odd prime $p$ and some $k \geq 0$. This gives clearly that $s(n) = (-1)^{N(n)} = 1$ if $r > 1$ unless $n = 2$ or $2p^k$ for some odd prime $p$. In the cases $n = 2p^k$ with $k \geq 0$, we have already seen that $s(n) = -1$.
Finally suppose $r = 1$ i.e., $n = p^k$ for some prime $p$. If $p$ is odd, we have already checked that $s(n) = -1$. If $p = 2$, then $s(2) = 1 = -1$ and $s(4) = -1$. But, in $\mathbf{Z}_{2^k}^*$ with $k \geq 3$, it can be seen after a little calculation that the only elements $a$ satisfying $a^2 = 1$ are $\pm 1, 2^{k-1} \pm 1$; so $N(2^k) = 4$ for all $k \geq 3$. In this case, we therefore have $s(2^k) = (-1)^{N(2^k)} = 1$.
Thus, we have proved the claim that $s(n) = 1$ if $\mathbf{Z}_n^*$ is not cyclic.

**Remarks.**
In what follows, perhaps a good third year undergraduate course in group theory is desirable to fully appreciate the results. From the above signature lemma, it becomes clear that $s(n) = 1$ (respectively $-1$) when there are at least two (respectively, exactly one) elements of order 2. This, in turn, is equivalent to the presence of more than one (respectively, exactly one) subgroup of order 2 in $\mathbf{Z}_n^*$. Looking at the product expression $\mathbf{Z}^*_{2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}} \cong \mathbf{Z}^*_{2^\alpha} \times \mathbf{Z}^*_{p_1^{\alpha_1}} \cdots \times \mathbf{Z}^*_{p_k^{\alpha_k}}$, it is clear that $\mathbf{Z}^*_{2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}}$ has a unique subgroup of order 2 if, and only if, the 2-Sylow subgroup is cyclic. Thus, $s(n) = -1$ or 1 according as to whether the 2-Sylow subgroup is cyclic or not. This points to the possibility of generalizing it to non-abelian groups where the 2-Sylow subgroups are cyclic. In fact, one can prove the following generalization.

**A non-abelian generalization :**
*Let $G$ be a finite (not necessarily abelian) group whose 2-Sylow subgroups are cyclic. Let $w \in G$ be any involution (that is, an element of order 2). Then, if $[G,G]$ denotes the commutator subgroup of $G$ (this consists of all finite products of elements of the form $xyx^{-1}y^{-1}$), the coset $w[G,G]$ is a nontrivial element of the quotient group $G/[G,G]$ and, the product of all the elements of $G$ taken in any order belongs to this coset (and is, hence, nontrivial). In particular, if $G$ is abelian with cyclic 2-Sylow subgroup, the product of all elements of $G$ is the unique involution in $G$.*

Note that the special case when $G = \mathbf{Z}_n^*$ is cyclic gives us $-1$ as in the signature lemma. We do not give the proof of this non-abelian version as it involves a few slightly advanced tools like the Schur-Zassenhaus theorem and also because we have been informed that it can be deduced from a still more general result due to A.R.Rhemtulla ('On a problem of L.Fuchs', Studia Scientifica Mathematica Hungarica, Vol. 4 (1969) 195-200).

**Address for correspondence :**
Stat-Math Unit
Indian Statistical Institute
8th Mile Mysore Road
Bangalore 560 059, India.
email : sury@isibang.ac.in