The Mathematical Association

259, London Road,
Leicester,
LE2 3BE
United Kingdom
Telephone (0116) 221 0013
Fax (0116) 212 2835

Registered Charity No. 313281

The Mathematical Gazette
Editor: Gerry Leversha

St Paul's School,
Lonsdale Road,
London
SW13 9JT
United Kingdom
e-mail: g.leversha@btinternet.com
10th May 2010

Urgent - requires immediate attention

Dear

I enclose a proof copy of your contribution to the July 2010 issue of *The Mathematical Gazette*. It has already been checked once by our proof-readers, and some minor rewordings, punctuation changes, etc. may have been made. Please check it carefully for errors, paying special attention to the diagrams, mathematical expressions, quotations from other sources and your name and address. If you have any essential changes, please mark them clearly in the margin in a contrasting colour, indicating the place in the text where the alteration is to be made. **Whether or not you have made alterations, please return the proof copy to me.**

The copyright for all contributions to the July 2010 issue of *The Mathematical Gazette*, including the right to reproduce them in all forms and media, should be assigned exclusively to The Mathematical Association. Please complete the copyright transfer form below and return it with your proof copy. If your article contains copyright materials from previously published sources, including your own published work, you must obtain written permission from the copyright owner and send the letter granting this permission to me. The Mathematical Association grants *you* permission to reproduce *your* contribution for non-profit making scholarly or educational use. You must obtain written permission from the Editor in Chief of The Mathematical Association, at 259 London Road, Leicester LE2 3BE, if you wish to reproduce your contribution in any publication.

Time is of the essence at this stage of the publication process. If I have not heard from you by Monday 24th May 2010, I will have to assume that you accept the article as it stands and that you agree to the terms of publication described in the paragraph above. **In an emergency you can fax the changes and reply form to Bill Richardson on 01343 860 450.**

Authors of articles, notes and matters for debate (*but not of letters, items in Feedback, or reviews*) may claim a free copy of the *Gazette.* All authors may claim an offprint of their contributions suitable for photocopying. If you wish to claim, please indicate on the form below.

Yours sincerely,

Gerry

Gerry Leversha

I hereby assign the copyright for all my contributions to the July 2010 issue of *The Mathematical Gazette* to The Mathematical Association.

Signed : . . . . Telephone: . . . .

Address: . . . .

Title(s) of item(s) . . . .

Please send a complimentary copy of the July 2010 *Gazette* ☐ (tick)

Please send an offprint of my contribution(s) to the July 2010 *Gazette* ☐ (tick)

94.13 Group theory lends a hand to number theory

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 $\mathbb{Z}_n^*$ of integers less than n and co-prime to n under multiplication modulo n. The classical Wilson's congruence $(p - 1)! \equiv -1 \pmod{p}$ for a prime p can be viewed as the assertion $\prod_{a \in \mathbb{Z}_p^*} a = p - 1$. 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, $p \mid (a^2 - 1)$ 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 $\prod_{a \in \mathbb{Z}_n^*} a$? The interesting result which emerges is embodied in the following signature lemma − so christened because it gives us the values ±1 depending on whether primitive roots mod n exist or not.

Signature lemma

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

Proof: If $\mathbb{Z}_n^*$ 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 $\mathbb{Z}_n^*$. But, since $s(n)$ above clearly has order 2, it follows that $s(n) = -1$ when $\mathbb{Z}_n^*$ is cyclic. Note that this also includes the trivial group $\mathbb{Z}_2^*$ as $1 = -1$ in that case.

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 $a \in \mathbb{Z}_n^*$ which satisfy $a^2 = 1$.

For a prime n this is Wilson's theorem.

We suppose n is arbitrary and $n > 2$. Now each such a in $\mathbb{Z}_n^*$ 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 $\mathbb{Z}_n^* / (\mathbb{Z}_n^*)^2$ as it is the order of the kernel of the squaring map on $\mathbb{Z}_n^*$. But, from the Chinese remainder theorem, note that under the isomorphism of $\mathbb{Z}_n^*$ with the product of $\mathbb{Z}_{p_i^{k_i}}^*$, where $n = \prod_i p_i^{k_i}$, the squares in $\mathbb{Z}_n^*$ 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 $N(n) = \prod_{i=1}^{r} N\left(p_i^{k_i}\right)$. Thus, if $r > 1$, then $N(n) \equiv 0 \bmod 4$ unless $n = 2p^k$ for some odd prime p and some $k \geqslant 0$. 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 $k \geqslant 0$ we have already seen that $s(n) = -1$.

Finally suppose $r = 1$, that is, $n = p^k$ 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 $\mathbb{Z}_{2^k}^*$ with $k \geqslant 3$ it can be seen after a little calculation that the only elements a satisfying $a^2 = 1$ are ± 1, $2^{k-1} \pm 1$; so $N\left(2^k\right) = 4$ for all $k \geqslant 3$. In this case we therefore have $s\left(2^k\right) = (-1)^{N(2^k)} = 1$.

Thus we have proved the claim that $s(n) = 1$ if $\mathbb{Z}_n^*$ 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 $\mathbb{Z}_n^*$. Looking at the product expression

$$\mathbb{Z}_{2^\alpha p_1^{\alpha_1} \ldots p_k^{\alpha_k}}^* \cong \mathbb{Z}_{2^\alpha}^* \times \mathbb{Z}_{p_1^{\alpha_1}}^* \times \ \ldots \ \times \mathbb{Z}_{p_k^{\alpha_k}}^*,$$

it is clear that $\mathbb{Z}_{2^\alpha p_1^{\alpha_1} \ldots p_k^{\alpha_k}}^*$ 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 generalising it* to non-abelian groups where the 2-Sylow subgroups are cyclic. In fact, one can prove the following generalisation.

A non-abelian generalisation

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 subgroups, the product of all elements of G is the unique involution in G.

Note that the special case when $G = \mathbb{Z}_n^*$ is cyclic gives us -1 as in the signature lemma. We do not give the proof of this non-abelian version as it

* Please clarify what the ‘it’ refers to.

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 [1].

Reference

1. A. R. Rhemtulla, On a problem of L. Fuchs, *Studia Scientifica Mathematica Hungarica,* **4** (1969) pp. 195-200.

B. SURY

Stat-Math Unit, Indian Statistical Institute, 8th Mile Mysore Road,
Bangalore 560 059, India

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