**Irish Math. Soc. Bulletin**
Number 94, Winter 2024, 99– 103
ISSN 0791-5578

# PROBLEMS

J.P. MCCARTHY

## Problems

We will ease into things with a problem from your erstwhile contributor, a version of which the previous editor felt was on the easy side, making it perhaps suitable for inviting undergraduates to engage with:

**Problem 94.1.** Let $X, Y$ be independent and identically distributed random variables with values in a finite group $G$. Let $H < G$ be a subgroup such that $\mathbb{P}[X \in H] \in (1/2, 1)$. Prove that

$$\mathbb{P}[XY \in H] < \mathbb{P}[X \in H].$$

More meatier group theory, this time courtesy of Des MacHale of University College Cork:

**Problem 94.2.** If $G$ is a group with centre $Z$ and $|G/Z| = n!$, for some integer $n > 1$, show that $G/Z$ is non-abelian.

The problem is stated for not-necessarily-finite groups, but solutions in the finite case are welcome. On the other hand, Des MacHale invites you to consider the following problem: for which numbers other than $n!$ does this result hold?

The following problem was provided by Anthony O'Farrell (Maynooth University) and Maria Roginskaya (Chalmers University of Technology):

**Problem 94.3.** A very large number of prizes are available for children at a big party thrown by a billionaire. The prizes are numbered $1, 2, 3, \ldots$, and are to be shared between a boy and a girl. Each boy at the party is given a card with a number in 1, 2, 3, ..., different for each boy, and the same is done for each girl, but it is possible that a boy will have the same number as some girl. There are $m$ boys and $n$ girls. A number $d \geq 1$ is specified, and this determines the rule for the allocation of prizes, as follows. The prize labelled $p$ is allocated to the first boy-girl partnership who present cards labelled $a$ and $b$, where $a + b = p$, and where $a$ differs from $b$ by no more than $d$. Having claimed a prize with some girl, a boy is free to claim others with other girls, and similarly for girls. Thus, as the party progresses, the children will repeatedly pair up and claim prizes, until all the prizes that can possibly be claimed are taken. Show that the number of prizes that can be claimed is less than $13\sqrt{mnd}$.

The following hint is provided: let $k$ be a nonnegative integer, and use induction on $k$ to get the best inequality you can for the number of prizes under the additional assumption that $mn \leq 2^k \cdot d$.

Received 13-12-2024
DOI: 10.33232/BIMS.0094.99.103.

## Solutions

Here are solutions to the problems from *Bulletin* Number 92.

The first problem was solved by the North Kildare Mathematics Problem Club, and the proposer, Des MacHale of University College Cork. We present the solution of Problem Club.

*Problem 92.1.* Show that the infinite cyclic group is not the full automorphism group of any group.

*Solution 92.1.* Suppose $\mathrm{Aut}(G)$ is cyclic. Then so is the subgroup of inner automorphisms, which is isomorphic to $G/Z$ (where $Z$ is the centre of $G$). Let $kZ$ generate $G/Z$. For $g, h \in G$ choose $m, n \in \mathbb{N}$ and $z, w \in Z$ with $g = k^m z$ and $h = k^n w$. Then

$$gh = k^m z k^n w = k^{m+n} zw = k^{m+n} wz = hg.$$

Therefore $G = Z$.

Since $G$ is abelian, $\tau : g \mapsto g^{-1}$ is an automorphism of $G$, and $\tau^2 = 1$. If we suppose, in addition, that $\mathrm{Aut}(G)$ is infinite or of finite odd order, then $\tau = 1$, i.e. each element of $g$ has $g^2 = 1$. Thus $G$ is a vector space over $\mathbb{Z}_2$. Each permutation of a basis of $G$ over $\mathbb{Z}_2$ gives an automorphism of $G$. At dimension greater than two, these permutations give non-commuting elements in $\mathrm{Aut}(G)$. At dimension two $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) = S_3$. It follows that $G$ has dimension at most one. But then $\mathrm{Aut}(\mathbb{Z}_2)$ is trivial, not infinite cyclic. □

The Problem Club leaves an aside: the proposer also posed the question of determining which finite cyclic groups could be $\mathrm{Aut}(G)$ for some group $G$.

The infinite cyclic group has the cyclic group of order two as its automorphism group. We have already seen that $\mathbb{Z}_n$ is never $\mathrm{Aut}(G)$ if $n > 1$ and $n$ is odd.

If $G$ is cyclic of order $m$, then $\mathrm{Aut}(G)$ is isomorphic to the multiplicative group of the ring of integers modulo $m$, and the order of $\mathrm{Aut}(G)$ is $\phi(m)$. This group is cyclic if and only if $\phi(m)$ is a product of distinct primes, so if and only if $m$ is a prime power $p^k$, and $(p-1)p^{k-1}$ is a product of distinct primes. Thus, whenever $p$ is prime and $p-1$ is square-free we have two groups $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ with cyclic automorphism groups, of respective orders $p-1$ and $p^2-p$. The first few orders of $\mathrm{Aut}(G)$ that arise this way are $1, 2, 6, 10, 22, 30$, and $2, 6, 42, 110, 486, 930$ (resulting from the primes $2, 3, 7, 11, 23, 31$).

For an abelian product group $G \times H$, the automorphism group contains $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$, and hence has at least two non-trivial involutions and is not cyclic, unless $\mathrm{Aut}(G)$ or $\mathrm{Aut}(H)$ is trivial. Thus the only finitely-generated abelian groups $G$ with cyclic $\mathrm{Aut}(G)$ are the cyclic examples just described, and their products with groups having only the identity automorphism..

It remains to consider abelian $G$ that are not finitely-generated.

Suppose $n > 0$, that $\mathbb{Z}_{2n}$ is isomorphic to $\mathrm{Aut}(G)$, and let $\sigma$ generate $\mathrm{Aut}(G)$. We know that $G$ is abelian, so $\tau : g \mapsto g^{-1}$ is an automorphism. There are two possibilities:

Case 1: $\tau = 1$. Then as before, $G$ has dimension at most one over $\mathbb{Z}_2$, so $\mathrm{Aut}(G)$ is trivial, a contradiction.

Case 2: $\tau \neq 1$. Then $\sigma^n = \tau$. Replacing $G$ by its quotient by the subgroup fixed by $\mathrm{Aut}(G)$, we may assume that each element of $G$ except 1 is moved by some automorphism, and hence is moved by $\sigma$. So each nonzero element $g \in G$ moves in a cycle of order $\alpha(g)$ dividing $2n$, under the action of $\mathbb{Z}_{2n}$. Let

$$\beta = \mathrm{lcm}\{\alpha(g) : g \in G\}.$$

Then $\beta|2n$ and $\sigma^\beta = 1$, so $\beta = 2n$. We can choose a finite number of elements $g_1,\ldots,g_m$ such that

$$2n = \mathrm{lcm}\{\alpha(g_1), \ldots, \alpha(g_m)\}.$$

Let $H = \langle g_1, \ldots, g_m\rangle$. Then $H$ is finitely-generated, and invariant under $\sigma$, and $\sigma|H$ has order $2n$. If $\sigma|H$ generates $\mathrm{Aut}(H)$, we have seen that $2n = p$ or $2n = p^2 - p$ for some prime $p$ such that $p - 1$ is square-free.

But does every automorphism of $H$ extend to an automorphism of $G$?

The second problem was solved by the North Kildare Mathematics Problem Club, and the proposer Andrei Zabolotskii of the Open University. We provide the solution of the Problem Club.

*Problem 92.2.* Let $A$ be a symmetric square matrix of even order over the ring of integers modulo 2. Suppose that all entries on the leading diagonal of $A$ are 0. Let $B$ be the square matrix obtained from $A$ by replacing each 0 entry with 1 and replacing each 1 entry with 0. Prove that $\det A = \det B$.

*Solution 92.2.* First note that $x^2 = x$ for $x$ in $\mathbb{Z}_2$. Also $+1 = -1$, so the sign of a permutation is 1 in $\mathbb{Z}_2$. Now let $A = [a_{ij}]$ be a symmetric $2n \times 2n$ matrix, entries in $\mathbb{Z}_2$, zero on the diagonal.

So $\det(A)$ is the sum

$$a_{1,\sigma(1)} \times \cdots \times a_{2n,\sigma(2n)}$$

where $\sigma$ ranges over all permutations of $1, .., 2n$. As $a_{ij} = a_{ji}$, we can cancel such a term with that arising from $\sigma^{-1}$, when $\sigma \neq \sigma^{-1}$. Thus only permutations that are involutions can survive. Also we can remove terms from involutions which fix one or more points (as they involve a diagonal entry in $A$). Finally, each term $a_{ij}$ will be matched by $a_{ji} = a_{ij}$. So their product can be recorded as $a_{ij}$.

Thus

$$\det(A) = \sum a_{i_1,i_2} \times \cdots \times a_{i_{2n-1},i_{2n}},$$

where $\{i_1, i_2\}, \{i_3, i_4\}, \ldots \{i_{2n-1}, i_{2n}\}$ ranges over all partitions of the set $\{1, 2, .., 2n\}$ into two-element subsets. There are $(2n)!/(2^n n!)$ such partitions, an odd number.

Let $J$ be the all 1's matrix. We need to compare $\det(A)$ with $\det(A + J)$. Analysing as above, we now have to sum over all involutions of $1, .., 2n$ (counting the identity as an involution).

$$\det(A + J) = \sum (1 + a_{i1,i2}) \times \cdots \times (1 + a_{i_{2n-1},i_{2n}}),$$

plus all sums involving fewer products of the same type. When these products are all expanded, the coefficient of a given product $a_{i_1,i_2}a_{i_3,i_4}\cdots a_{i_{2r-1},i_{2r}}$ is (equal modulo 2 to) the number of involutions of $\{1, \ldots, 2n\}$ that fix $\{i_1, i_2, i_3, i_4, \ldots, i_{2r-1}, i_{2r}\}$. When $r < n$, the coefficient equals the number of involutions of a set of $2n - 2r$ elements, which is even, so zero modulo 2. (This applies even to the empty product, 1, so there is an even number of 1's). Hence the only terms that survive are those with $r = n$, and these sum to $\det(A)$. □

Readers were asked to consider the more challenging question of whether or not the characteristic polynomials of $A$ and $B$ are equal. The Problem Club provided a "leisurely version" of the above proof which was a wonderful interplay between orbits, involutions, and fixed points. The approach also spoke to the case of matrices with entries in a commutative ring $R$ with identity, where key was the language of a matrix in $M_n(R)$ as a function $x : \mathcal{P}_1([n]) \sqcup \mathcal{P}_2([n]) \to R$. The technology in the leisurely version helped answer the challenging question in the positive: indeed the characteristic polynomials of $A$ and $B$ are equal.

The third problem was solved by the North Kildare Mathematics Problem Club; the proposer, Tran Quang Hung of the Vietnam National University at Hanoi, Vietnam; Kee-Wai Lau of Hong Kong, China; and your erstwhile contributor. Here is one of those solutions:

*Problem 91.3.* For $x > 0$, let $\mu(x)$ denote the $\ell_\infty$-norm of the sequence

$$u_n(x) = \frac{x^n}{n^n}, \quad n = 1, 2, \ldots .$$

Determine

$$\lim_{x\to\infty} \frac{\log \mu(x)}{x}.$$

*Solution 92.3.* For fixed $x > 1$, extend the sequence $\mu_n(x)$ to a function $f_x : [1, \infty) \to (0, \infty)$:

$$f_x(y) = \frac{x^y}{y^y}.$$

It is strictly positive as $f_x(y) = \exp\left(\log\left(\frac{x}{y}\right) y\right)$. Its derivative with respect to $y$ is:

$$\frac{d}{dy}(f_x(y)) = f_x(y)\left(\log\left(\frac{x}{y}\right) - 1\right).$$

Note as $f_x(y)$ is strictly positive, this derivative is strictly positive on $[1, x/e)$, and strictly negative on $(x/e, \infty)$.

It follows that for fixed $x > 1$, $\mu(x)$ attains its maximum at $\lfloor x/e \rfloor$ or $\lceil x/e \rceil$. Therefore we know that for some $z_x \in (-1, 1)$ the maximum occurs at

$$\frac{x}{e} + z_x.$$

We calculate, using the fact that $x$ can be chosen large enough to make each of the manipulations valid:

$$\mu(x) = \left(\frac{x}{\frac{x}{e} + z_x}\right)^{\frac{x}{e}+z_x}.$$

Then,

$$\begin{aligned}
\log \mu(x) &= \left(\frac{x}{e} + z_x\right) \log\left(\frac{x}{\frac{x}{e} + z_x}\right) \\
&= \frac{1}{e}(x + ez_x) \log\left(e \cdot \frac{x}{x + ez_x}\right) \\
&= \frac{1}{e}(x + ez_x)\left[\log e + \log\left(\frac{x}{x + ez_x}\right)\right],
\end{aligned}$$

and so

$$\frac{\log \mu(x)}{x} = \frac{1}{e}\left(1 + \frac{ez_x}{x}\right)\left[1 + \log\left(\frac{1}{1 + \frac{ez_x}{x}}\right)\right].$$

As a consequence,

$$\lim_{x\to\infty} \frac{\log \mu(x)}{x} = \frac{1}{e} \times 1 \times (1 + \log(1)) = \frac{1}{e}. \qquad \square$$

We invite readers to submit problems and solutions. Please email submissions to `imsproblems@gmail.com` in any format (but preferably LaTeX). Submissions for the summer Bulletin should arrive before the end of April, and submissions for the winter Bulletin should arrive by October. The solution to a problem is published two issues

after the issue in which the problem first appeared. Please include solutions to any problems you submit, if you have them.

Finally, I would like to thank Ian Short for his many, many years of service to this problem page. With your help, we can continue Ian's great work.

Department of Mathematics, Munster Technological University