# Problemen

Problem Section

**Edition 2008/3**

We received submissions from Rik Bos (Bunschoten), Rob van der Waall (Huizen), Tejaswi Navilarekallu (Amsterdam), Rohith Varma (Chennai), the Fejéntaláltuka Szeged Problem Group (Szeged), Peter Bruin (Leiden), Noud Aldenhoven & Frans Clauwens (Nijmegen), F.N. Aliyev & Y.N. Aliyev (Baku), Sander Kupers (Utrecht).
We regret that in the last issue we forgot to mention Paolo Perfetti's correct solution to problem 2008/1-C.

**Problem 2008/3-A** Let $a$ and $b$ be integers. Show that the following are equivalent:
1. $n$ divides $a^n - b^n$ for infinitely many positive integers $n$,
2. $|a - b| \neq 1$.

**Solution** This problem was solved by Noud Aldenhoven & Frans Clauwens, Rik Bos, Tejaswi Navilarekallu, F.N. Aliyev & Y.N.Aliyev, the Fejéntaláltuka Szeged Problem Group and Rob van der Waall. The book token goes to Noud Aldenhoven & Frans Clauwens.
The following solution is based on several of these submissions.
First we show that (1) implies (2). So assume that there exists an $n > 1$ that divides $(a+1)^n - a^n$. Since $n$ divides the difference of an even and an odd number it is odd. Let $p$ be the smallest prime dividing $n$. Then the numbers $p-1$ and $n$ are coprime, so there exist integers $s$ and $t$ with $sn + t(p-1) = 1$.
Since $p$ does not divide $a$ nor $a+1$, Fermat's little theorem says that $a^{p-1}$ and $(a+1)^{p-1}$ are both congruent to 1 modulo $p$, so in particular:

$$(a+1)^{t(p-1)} \equiv a^{t(p-1)} \pmod{p}.$$

Since $p$ divides $(a+1)^n - a^n$ we also have

$$(a+1)^{sn} \equiv a^{sn} \pmod{p}.$$

Combining both congruences gives

$$(a+1)^{sn+t(p-1)} \equiv a^{sn+t(p-1)}.$$

Hence $a \equiv a+1$, which is a contradiction.
For the other implication, if $|a-b| \neq 1$ then there exists a prime number $p$ such that $p$ divides $a-b$. But in that case is not hard to show that for all positive integers $k$

$$p^k \text{ divides } a^{p^k} - b^{p^k},$$

which gives infinitely many $n$ with the desired property.

**Problem 2008/3-B** Let $G$ be a finite group and $a$ be an element of $G$. Show that the number of elements $g \in G$ that satisfy both $ga \neq ag$ and $ga^2 = a^2g$ is divisible by 4.

**Solution** This problem was solved by Rik Bos, Rob van der Waall, Tejaswi Navilarekallu, Rohith Varma, the Fejéntaláltuka Szeged Problem Group and Peter Bruin. The book token goes to Rik Bos. The shortest solution we received is the following one-line proof by Peter Bruin:
The map $g \mapsto ag^{-1}$ induces a free action of a cyclic group of order 4 on the set of elements of $G$ that commute with $a^2$ but not with $a$.
Rik Bos proved a generalisation, namely he showed:
Let $G$ be a finite group, $a$ an element of $G$ and $p$ be a prime number. Then $p^2$ divides the number of elements of $G$ that commute with $a$ if and only if it divides the number

*Eindredactie:*
*Lenny Taelman, Johan Bosman*
*Redactieadres:*
*Problemenrubriek NAW*
*Mathematisch Instituut*
*Postbus 9512*
*2300 RA Leiden*
*problems@nieuwarchief.nl*

Oplossingen | Solutions

of elements of $G$ that commute with $a^p$. It is not difficult to deduce the original problem from this statement.

---

**Problem 2008/3-C** Let $p$ be an odd prime number and $A$ and $B$ two $n \times n$ matrices with entries in $\mathbf{Z}$ such that $A^p = B^p = 1$, and such that the rank of $A - B$ is 1. Show that $n \geq p$.

**Solution** This problem was solved by Rik Bos and Tejaswi Navilarekallu. The book token goes to Tejaswi Navilarekallu. The following solution is based on both submissions.
Assume that $n < p$. An $n$ by $n$ matrix $M$ with $M^p = 1$ is either the identity matrix, or has $(x^p - 1)/(x - 1)$ as characteristic polynomial. In the latter case $n$ is necessarily $p - 1$. So if $n < p - 1$ then $A = B = 1$ which contradicts the hypothesis on the rank of $A - B$.
Hence we may assume that $n = p - 1$ and that $A \neq 1$. We have to consider two cases: $B = 1$ and $B \neq 1$.
First case: $B = 1$. Define $\zeta$ to be the $p$-th root of unity $e^{2\pi i/p}$. The eigenvalues of $A - 1$ are $\zeta - 1, \zeta^2 - 1, \ldots, \zeta^{p-1} - 1$. So the rank of $A - B = A - 1$ is $p - 1$ which is a contradiction.
Second case: $B \neq 1$. In this case there is an invertible matrix $Q$ with rational entries and with $B = Q^{-1}AQ$. Define $C$ to be the matrix $AQ - QA$. Since $C = Q(A - B)$, it has rank 1.
*Claim:* For all vectors $v$ and for integers $i$ we have the equality $CA^iCv = 0$.
Proof of the claim: the rank of $CA^i$ is at most 1 and we have

$$\operatorname{trace}(CA^i) = \operatorname{trace}(AQA^i - QA^{i+1}) = \operatorname{trace}(A \cdot QA^i) - \operatorname{trace}(QA^i \cdot A) = 0,$$

from which we deduce that $CA^i$ has no non-zero eigenvalues. Since the rank of $CA^i$ is at most one, $CA^iw$ is an eigenvector of $CA^i$ for all vectors $w$, so in particular, taking $w = A^{-i}v$, we find that $Cv$ is an eigenvector of $CA^i$. Hence $CA^iCv = 0$, which proves the claim.
Now let $v \in \mathbf{Q}^n$ be such that $Cv \neq 0$. Let $W$ be the vector space spanned by $Cv, ACv, A^2Cv, \ldots$ Then $W$ is a non-zero $A$-invariant subspace of $\mathbf{Q}^n$. Since $W$ is contained in the kernel of $C$, the dimension of $W$ is strictly smaller then $n$. It follows that the characteristic polynomial of $A$ is reducible over $\mathbf{Q}$, which is a contradiction.