Canad. Math. Bull. Vol. **15** (3), 1972

PROBLEMS AND SOLUTIONS

This department welcomes problems believed to be new. Solutions should accompany proposed problems.

Send all communications concerning this department to

PROBLÈMES ET SOLUTIONS

Cette section a pour but de présenter des problèmes inédits. Les problèmes proposés doivent être accompagnés de leurs solutions.

Veuillez adresser les communications concernant cette section à

E. C. Milner, Problem Editor
Canadian Mathematical Bulletin
Department of Mathematics
University of Calgary
Calgary 44, Alberta

PROBLEMS FOR SOLUTION

P.203. Prove the group identity

$$[x, y, \bar{y}]^{\bar{x}}[y, \bar{x}, x]^{\bar{y}}[\bar{x}, \bar{y}, y]^{x}[\bar{y}, x, \bar{x}]^{y} = 1,$$

where $\bar{x}=x^{-1}$, $x^y=\bar{y}xy$ and the commutator $[x, y]=\overline{xy}xy$ and $[x, y, z]=[[x, y], z]$.

J. M. Gandhi and D. Kreiling,
Western Illinois University

P.204. Let R be a ring with 1. Recall that (i) $e \in R$ is *idempotent* if $e^2=e$, (ii) $u \in R$ is a *unit* if there exists $v \in R$ such that $uv=vu=1$. Show that, if $1+1$ is a unit of R, then any idempotent is the sum of two units.

R. Raphael,
Sir George Williams University

P.205. Find the integer solutions of the diophantine equation $y^2=x(x+y-1)$.

Guy A. R. Guillot,
Montreal, Quebec

P.206. Let $(i_1, \ldots, i_r)$ be a partition of the integer k, i.e. the i_j are positive integers and $i_1+\cdots+i_r=k$. Prove that

$$N = \binom{2k+1}{i_1}\binom{2k+1}{i_2}\cdots\binom{2k+1}{i_r}$$

is divisible by $2k+1$.

Jacques Troué,
McGill University

P.207. A latin square (a_{ij}) is *idempotent* if $a_{ii}=i$. Show that there are $n-2$ mutually orthogonal idempotent latin squares (cf. H. J. Ryser, Combinatorial Mathematics) of order n if and only if there is a projective plane of order n.

WILLIAM JONSSON,
McGILL UNIVERSITY

P.208. If $\tau(n)$ and $\sigma(n)$ denote respectively the number of and the sum of the divisors of n, show that

$$\prod_{d/n} d^{d-n/d} = n^{\sigma(n)}e^{-2nr\tau(n)},$$

where $0 \leq r \leq e^{-1}$.

C. S. VENKATARAMAN,
SREE KERALA VARMA COLLEGE, INDIA

SOLUTIONS

P.180. Prove that in a groupoid (i.e. a set with a binary operation) satisfying the identity

$$(y(xy))((xy)(y(xy))) = x$$

every equation $xb=a$ has a unique solution.

N. S. MENDELSOHN,
UNIVERSITY OF MANITOBA

Solution by Stanley Wagon, McGill University. The unique solution to $xb=a$ is $x=((ba)(a(ba)))$. To see this put $y=ba$ and $x=a$ in the given identity to get $((ba)(a(ba)))((a(ba))((ba)(a(ba))))=a$ or $((ba)(a(ba)))b=a$. That this solution is unique follows from the fact that $xb=a$ implies that $x=(b(xb))((xb)(b(xb))=(ba)(a(ba))$.

Also solved by Paul Milnes, Univ. of Western Ontario; A. G. Heinicke, Univ. of Western Ontario; R. Padmanabhan, Univ. of Manitoba; Arthur S. Finbow, Dalhousie Univ.; Helen F. Cullen, Univ. of Massachusetts; R. D. Giri, Aligarh Muslim University, India; P. Ramankutty, Univ. of Auckland, New Zealand, and Lia Chang-Der, Ohio State University.

P.181. Show that there does not exist a variety of groupoids (i.e. a family closed under subgroupoids, cartesian products and homomorphisms) with the property that for any groupoid of the variety any two distinct elements generate a subgroupoid of order 6 (except for the vacuous case of a variety containing only one groupoid with exactly one element). Note that such varieties can be shown to exist if 6 is replaced by any of 2, 3, 4, 5, 7, 8, 9.

N. S. MENDELSOHN,
UNIVERSITY OF MANITOBA

https://doi.org/10.1017/S0008439500031465 Published online by Cambridge University Press

Solution by the Proposer. If such a variety existed there would be a groupoid G in the variety with exactly six elements. The groupoid $G\times G$ is in the variety and any two of its elements generate a subgroupoid of order 6. This implies that there is a B.I.B. design with parameters $v=36$, $b=42$, $r=7$, $k=6$, $\lambda=1$, a contradiction since an affine plane of order 6 does not exist.

One other (incorrect) solution was received.

P.182. Find the number of solutions of the congruence in kn variables

$$\sum_{i=1}^{n}\prod_{j=1}^{k} x_{ij} \equiv 0 \pmod{p},$$

where p is a prime.

L. J. Mordell, St. John's College, Cambridge, and
The University of Calgary

Solution by Kenneth S. Williams, Carleton University. Let p be a prime. For any integer a we have

$$\sum_{x=0}^{p-1}\exp(2\pi iax/p) = \begin{cases} p, & \text{if } a \equiv 0 \pmod{p}, \\ 0, & \text{if } a \not\equiv 0 \pmod{p}, \end{cases} \tag{1}$$

as the left hand side of (1) is a geometric progression. Now if $a\not\equiv 0 \pmod{p}$ and $k\geq 2$ we have using (1)

$$\begin{aligned} \sum_{x_1,\ldots,x_k=0}^{p-1} \exp(2\pi iax_1\cdots x_k/p) &= \sum_{x_1,\ldots,x_{k-1}=0}^{p-1}\left\{\sum_{x_k=0}^{p-1}\exp(2\pi i(ax_1\cdots x_{k-1})x_k/p)\right\} \\ &= p\sum_{\substack{x_1,\ldots,\ k-1=0 \\ x_1\ldots x_{k-1}=0}}^{p-1} 1 \\ &= p\{p^{k-1}-(p-1)^{k-1}\}, \end{aligned}$$

as the last sum is just the number of $(k-1)$-tuples $(x_1,\ldots,x_{k-1})$ with at least one zero entry. Putting this result together with (1) we have for $a\not\equiv 0 \pmod{p}$ and $k\geq 1$

$$\sum_{x_1,\ldots,x_k=0}^{p-1} \exp(2\pi iax_1\cdots x_k/p) = p\{p^{k-1}-(p-1)^{k-1}\}. \tag{2}$$

Now let $a_1,\ldots,a_n$ be n integers *not* divisible by p, a_0 any integer, and $k_1,\ldots,k_n$ integers ≥ 1. We determine the number $N_p(n, \mathbf{k}, \mathbf{a}, a_0)$ of solutions of the congruence

$$\sum_{j=1}^{n} a_jx_{j1}\cdots x_{jk_j}+a_0 \equiv 0 \pmod{p},$$

where we have written $\mathbf{k}$ for $(k_1,\ldots,k_n)$ and $\mathbf{a}$ for $(a_1,\ldots,a_n)$.

From (1) we have

$$
\begin{aligned}
&N_p(n, \mathbf{k}, \mathbf{a}, a_0)\\
&= \sum_{x_{11},\dots,x_{1k_1},x_{21},\dots,x_{nk_n}=0}^{p-1} \left\{\frac{1}{p}\sum_{t=0}^{p-1} \exp\left(2\pi i t\left(\sum_{j=1}^{n} a_j x_{j1}\cdots x_{jk_j}+a_0\right)\Big/ p\right)\right\}\\
&= p^{k_1+\cdots+k_n-1}+\frac{1}{p}\sum_{t=1}^{p-1}\exp(2\pi i t a_0/p)\prod_{j=1}^{n}\left(\sum_{x_{j1},\dots,x_{jk_j}=0}^{p-1}\exp(2\pi i t a_j x_{j1}\cdots x_{jk_j}/p)\right)\\
&= p^{k_1+\cdots+k_n-1}+p^{n-1}\prod_{j=1}^{n}(p^{k_j-1}-(p-1)^{k_j-1})\sum_{t=1}^{p-1}\exp(2\pi i t a_0/p) \quad \text{(using (2))}\\
&= \begin{cases} p^{k_1+\cdots+k_n-1}+p^{n-1}(p-1)\prod_{j=1}^{n}(p^{k_j-1}-(p-1)^{k_j-1}), & \text{if } a_0\equiv 0 \pmod p,\\ p^{k_1+\cdots+k_n-1}-p^{n-1}\prod_{j=1}^{n}(p^{k_j-1}-(p-1)^{k_j-1}), & \text{if } a_0\not\equiv 0 \pmod p.\end{cases}
\end{aligned}
$$

The number asked for by Mordell is therefore

$$N_p(n, k\mathbf{1}, \mathbf{1}, 0) = p^{nk-1}+p^{n-1}(p-1)(p^{k-1}-(p-1)^{k-1})^n.$$

Also solved by E. M. Charles, Calgary, and L. Carlitz, Duke Univ. Professor Carlitz obtained a similar generalization (with $\mathbf{a}=\mathbf{1}$) and gave the following two references for more general results of this kind: (1) *The number of solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **38** (1952), 515–519; (2) *The number of solutions of some special equations in a finite field*, Pacific J. Math. **4** (1954), 207–217.

P.183. For which cardinals m, n is the following statement true: If $\mathscr{F}$ is a set of sets, $|\mathscr{F}|=m$, then there is a set X such that $|X|=n$ and $F\cap X\neq F'\cap X$ if F, F' are distinct members of $\mathscr{F}$.

J. P. Jones, E. C. Milner and N. Sauer,
University of Calgary

Solution by E. C. Milner, University of Calgary. We remark first that if X distinguishes the members of $\mathscr{F}$ (i.e. $F_1, F_2\in\mathscr{F}$, $F_1\neq F_2\Rightarrow F_1\cap X\neq F_2\cap X$), then so also does $X\cup Y$ for an arbitrary set Y. It follows that all one is really interested in is the *least* cardinal $n=f(m)$ such that: if $\mathscr{F}$ is any set of sets with $|\mathscr{F}|=m$, then there is an n-element set X which distinguishes the members of $\mathscr{F}$.

If $\mathscr{F}$ is a family of m mutually disjoint sets and $|X|<m-1$, then there are two members of $\mathscr{F}$ which have the same (empty) intersection with X. Hence, $f(m)\geq m-1$. We will prove that equality holds.

First a simple lemma.

LEMMA. *Let A be a finite, nonempty set and let $\mathscr{F}$ be a set of subsets of A such that whenever $x \in A$ there are $F_1, F_2 \in \mathscr{F}$ such that*

$$x \notin F_1, \qquad F_2=\{x\} \cup F_1. \tag{1}$$

Then $|\mathscr{F}|>|A|$.

Proof. We use induction on $|A|$. For $|A|=1$ the result is obvious. Assume $|A|>1$ and fix some $a \in A$. If $F \in \mathscr{F}$, put $F'=F\diagdown\{a\}$ and let $\mathscr{F}'=\{F':F \in \mathscr{F}\}$. For $x \in A\diagdown\{a\}$ there are F_1, F_2 which satisfy (1) and which therefore also satisfy $x \notin F_1'$, $F_2'=\{x\} \cup F_1'$. Then, by the induction hypothesis, $|\mathscr{F}'|>|A\diagdown\{a\}|$. Since $\mathscr{F}$ contains two sets U, V with $a \notin U$, $V=\{a\} \cup U$, it follows that $|\mathscr{F}|\geq|\mathscr{F}'|+1>|A|$. This proves the lemma.

Now let m be a positive integer and let $\mathscr{F}$ be a set of m sets. We want to show that there is a distinguishing set X with $|X|\leq m-1$.

Case 1. $\cup\mathscr{F}$ is finite. In this case we use induction on $|\cup\mathscr{F}|$. If $|\cup\mathscr{F}|<m$, put $X=\cup\mathscr{F}$. Now suppose that $|\cup\mathscr{F}|\geq m$. For each $x \in \cup\mathscr{F}$, let $\mathscr{F}_x=\{F\diagdown\{x\}: F \in \mathscr{F}\}$. If $|\mathscr{F}_x|=|\mathscr{F}|$, then the result is immediate, for $\mathscr{F}_x$ has a distinguishing set X with $|X|<m$ by the induction hypothesis, and X also distinguishes between the sets in $\mathscr{F}$. Therefore, we can assume that for each $x \in \cup\mathscr{F}$ there are $F_1, F_2 \in \mathscr{F}$ such that (1) holds. By the lemma it follows that $m=|\mathscr{F}|>|\cup\mathscr{F}|\geq m$, a contradiction.

Case 2. $\cup\mathscr{F}$ is arbitrary. Let $\mathscr{F}=\{F_1, \ldots, F_m\}$ and, for each set of indices $N \subset \{1, \ldots, m\}$, let

$$A_N = \bigcap_{i\in N} F_i\diagdown\bigcup_{i\notin N} F_i.$$

If $A_N=\phi$ let $X_N=\phi$, and if $A_N\neq\phi$ let X_N be a one-element subset of A_N. Put

$$B_i = \bigcup_{i\in N\subset\{1,\ldots,m\}} X_N \qquad (1 \leq i \leq m).$$

The sets $B_1, \ldots, B_m$ are finite and distinct and so, by Case 1, there is a set X with fewer than m elements which distinguishes between these sets. Suppose $X \cap B_i\diagdown X \cap B_j\neq\phi$. Then there is $N \subset \{1, \ldots, m\}$ such that $i \in N$, $j \notin N$ and $X_N\neq\phi$. Then $X_N \subset X \cap F_i\diagdown X \cap F_j\neq\phi$, i.e. X also distinguishes the members of $\mathscr{F}$.

Finally we consider the case when m is infinite. Suppose $\mathscr{F}=\{F_\nu:\nu \in I\}$, where I is an index set of cardinal power m. Let $A_{\mu\nu}=F_\mu\diagdown F_\nu$ $(\mu, \nu \in I)$. If $A_{\mu\nu}=\phi$ put $X_{\mu\nu}=\phi$, and if $A_{\mu\nu}\neq\phi$ let $X_{\mu\nu}$ be a one-element subset of $A_{\mu\nu}$. Put

$$B_\mu = \bigcup_{\nu\neq\mu} X_{\mu\nu} \quad (\mu \in I), \qquad X = \bigcup_{\mu\in I} B_\mu.$$

The set X has power at most m $(=m-1)$ and distinguishes the members of $\mathscr{F}$.