THE UNIVERSITY OF SYDNEY

# Sydney University Mathematical Society Problem Competition 2013

**1.** Alice, Bess and Cath want to host seven parties in 2014, occurring on the seven different days of the week. Alice writes down a list of seven dates in 2014, in which no day of the week is repeated. Bess crosses out the first date on Alice's list (a Wednesday) and replaces it with a randomly chosen alternative date, without looking at the rest of the list. Cath now considers each of the other dates on the list in turn, starting from the second one. If its day of the week has not appeared earlier in the list, she leaves the date unchanged; and if its day of the week has appeared earlier, she replaces it with a randomly chosen date whose day of the week has not appeared earlier. What is the probability that she changes the last date on the list?

**Solution.** The year 2014 will start on a Wednesday (and is not a leap year!), so it will contain 53 Wednesdays and 52 of each other day of the week. Since all non-Wednesday days of the week are equivalent, we can assume that the last date on Alice's list is a Sunday.

Notice that if Bess chooses another Wednesday to replace the first date, then Cath makes no changes to the rest of the list. Otherwise, Cath must choose a Wednesday at some point. Moreover, since Cath only changes dates whose day of the week has been taken by her (or Bess's) previous change, from the point at which she first chooses a Wednesday there are no further changes for her to make. Thus, the scenarios in which the last date on the list is changed are exactly those in which either Bess or Cath chooses a Sunday before the first choice of a Wednesday.

Since Bess definitely changes Alice's first date, there are 52 possible Wednesdays she might replace it with. So the probability that she writes down a Wednesday is $1/7$, the same as the probability that she writes down a Sunday. With probability $5/7$ she writes down some other day of the week, and then the determining factor is Cath's choices. When Cath has to make a choice in which both Wednesdays and Sundays are open to her, Wednesdays predominate over Sundays in the ratio 53:52 (note that the question did not rule out Alice's original Wednesday as a possible choice for Cath). So the probability that she chooses a Sunday before her first choice of a Wednesday is $52/105$. Therefore the overall probability we are seeking is

$$\frac{1}{7} + \frac{5}{7} \times \frac{52}{105} = \frac{73}{147}.$$

**2.** David is also planning a party, at which there are to be $26$ guests. Considering that a triple of guests has 'social potential' if it contains a pair who have met each other before and also a pair who haven't met each other before, he wants at least half of all the $\binom{26}{3}$ triples to have social potential. What is the smallest number of previously-acquainted pairs that could possibly be compatible with this requirement?

**Solution.** In the terminology of graph theory, we are considering simple graphs with $26$ vertices, and we want to know the minimal number of edges among all graphs with the property that at least half of the triples of vertices contain either $1$ or $2$ edges.

Take a simple graph with 26 vertices, labelled $1, \cdots, 26$. Let $d_i$ ($1 \le i \le 26$) denote the degree (= number of adjacent vertices) of vertex $i$. Then $\sum_{i=1}^{26} d_i = 2e$ where $e$ is the number of edges.

Let $t$ be the number of triples of vertices that contain either 1 or 2 edges. Each such triple gives rise to exactly two ordered triples $(i, j, k)$ such that vertex $i$ is adjacent to vertex $j$ but not to vertex $k$. For a fixed $i$, the number of ways to choose such $j$ and $k$ is clearly $d_i(25 - d_i)$. Hence

$$t = \frac{1}{2}\sum_{i=1}^{26} d_i(25 - d_i) = 25e - \frac{1}{2}\sum_{i=1}^{26} d_i^2. \tag{1}$$

Now we can show that the answer to the question is 65. Firstly, it is easy to see that it is possible to have a graph with 26 vertices in which every vertex has degree 5; in this case $e = 65$ and equation (1) gives $t = 25 \times 65 - 13 \times 25 = 1300$, so exactly half of the $\binom{26}{3} = 2600$ triples of vertices contain either 1 or 2 edges.

Conversely, suppose that $t \ge 1300$. Then (1) gives

$$\sum_{i=1}^{26} d_i^2 \le 50e - 2600.$$

On the other hand, the Cauchy–Schwarz inequality implies that

$$26\sum_{i=1}^{26} d_i^2 \ge (\sum_{i=1}^{26} d_i)^2 = 4e^2.$$

Putting these inequalities together we find that

$$e^2 - 325e + 16900 \le 0.$$

The left-hand side factorizes as $(e - 65)(e - 260)$, so we deduce that $65 \le e \le 260$.

**3.** Define a sequence by the initial value $b_1 = 3$ and the recurrence relation $b_{n+1} = b_n^2 - 2$ for $n \ge 1$. Evaluate the limit $\lim\limits_{m\to\infty} \dfrac{b_m}{b_1 b_2 \cdots b_{m-1}}$.

**Solution.** Clearly $b_n > 2$ for all $n$, so we can define positive real numbers $t_n$ uniquely by the condition that $b_n = 2\cosh t_n$. Then the recurrence becomes $\cosh t_{n+1} = 2\cosh^2 t_n - 1 = \cosh(2t_n)$, impying that $t_{n+1} = 2t_n$ for all $n \ge 1$, so $t_n = 2^{n-1}t_1$. This means that

$$b_n = \frac{\sinh(2t_n)}{\sinh t_n} = \frac{\sinh(2^n t_1)}{\sinh(2^{n-1}t_1)},$$

so the product $b_1 b_2 \cdots b_{m-1}$ telescopes, leaving

$$\frac{b_m}{b_1 b_2 \cdots b_{m-1}} = 2\sinh(t_1)\frac{\cosh(2^{m-1}t_1)}{\sinh(2^{m-1}t_1)}.$$

Since $\lim_{x\to\infty} \frac{\cosh x}{\sinh x} = 1$, the answer is

$$2\sinh t_1 = \sqrt{b_1^2 - 4} = \sqrt{5}.$$

**4.** Find the determinant of the $n \times n$ matrix whose $(i, j)$-entry is $i$ if $i \neq j$, and is $i + 1$ if $i = j$.

**Solution.** Let this matrix be $M_n$, and let $I_n$ be the $n \times n$ identity matrix. Then $M_n - I_n$ is the matrix where the $i$th row is $(i, i, \cdots, i)$. Thus $M_n - I_n$ has rank 1 and its null space (kernel) is $(n-1)$-dimensional, consisting of all vectors for which the coordinates sum to zero. This means that 1 is an eigenvalue of $M_n$ with multiplicity at least $n - 1$. Since the trace of $M_n$ is $\sum_{i=1}^{n} i + 1 = \frac{n^2+3n}{2}$, and the trace is the sum of the eigenvalues, the final eigenvalue of $M_n$ is $\frac{n^2+3n}{2} - (n-1) = \frac{n^2+n+2}{2}$. Therefore the determinant, the product of the eigenvalues, is $\frac{n^2+n+2}{2}$.

**5.** Fix an integer $n > 1$ and consider the permutations of the set $\{1, 2, \cdots, n\}$. Say that such a permutation $\sigma$ is *self-inverse* if $\sigma(\sigma(i)) = i$ for all $1 \leq i \leq n$. Say that $\sigma$ is *modest* if $\sigma(i) > \min\{\sigma(i+1), \sigma(i+2)\}$ for all $1 \leq i \leq n-2$. Prove that the number of self-inverse permutations equals the number of modest permutations.

**Solution.** Let $a_n$ and $b_n$ denote the number of self-inverse and modest permutations, respectively, of $[n] = \{1, 2, \cdots, n\}$. We have $a_2 = b_2 = 2$ and $a_3 = b_3 = 4$ by an easy count. It is therefore enough to show that the two numbers satisfy the same recurrence relation, namely

$$a_n = a_{n-1} + (n-1)a_{n-2} \text{ and } b_n = b_{n-1} + (n-1)b_{n-2} \text{ for } n \geq 4.$$

To prove $a_n = a_{n-1} + (n-1)a_{n-2}$, note that a self-inverse permutation $\sigma$ of $[n]$ either has $\sigma(n) = n$ or $\sigma(n) < n$. If $\sigma(n) = n$, then the restriction of $\sigma$ to $[n-1]$ is a self-inverse permutation, and each such arises once only in this way, so the number of self-inverse $\sigma$ with $\sigma(n) = n$ is $a_{n-1}$. If $\sigma(n) < n$, then there are $n - 1$ possibilities for $\sigma(n)$. Whatever $\sigma(n)$ is, the restriction of $\sigma$ to $[n-1] \setminus \{\sigma(n)\}$ is a self-inverse permutation, and each such arises once only in this way, so the number of self-inverse $\sigma$ with $\sigma(n) < n$ is $(n-1)a_{n-2}$.

To prove $b_n = b_{n-1} + (n-1)b_{n-2}$, note that a modest permutation $\sigma$ cannot have $\sigma(i) = 1$ for $i \leq n-2$, so it must have either $\sigma(n) = 1$ or $\sigma(n-1) = 1$. If $\sigma(n) = 1$, then we obtain a modest permutation $\tau$ of $[n-1]$ by setting $\tau(i) = \sigma(i) - 1$, and each such arises once only in this way, so the number of modest $\sigma$ with $\sigma(n) = 1$ is $b_{n-1}$. If $\sigma(n-1) = 1$, then there are $n-1$ possibilities for $\sigma(n)$ (the modesty condition $\sigma(n-2) > \min\{\sigma(n-1), \sigma(n)\}$ is automatic). Whatever $\sigma(n)$ is, we obtain a modest permutation $\tau$ of $[n-2]$ by setting $\tau(i) = \sigma(i) - 1$ if $\sigma(i) < \sigma(n)$ and $\tau(i) = \sigma(i) - 2$ if $\sigma(i) > \sigma(n)$, and each such arises once only in this way, so the number of modest $\sigma$ with $\sigma(n) = 1$ is $(n-1)b_{n-2}$.

**Alternative solution.** We can construct a bijection between self-inverse and modest permutations of $\{1, 2, \cdots, n\}$ as follows. Given a self-inverse permutation $\sigma$, write it in cycle notation with the 1-cycles included, each 2-cycle written with the smaller element first, and the cycles put in decreasing order of their smallest element. For example, when $n = 7$ we might consider the self-inverse permutation $(7)(4)(3\ 6)(2\ 5)(1)$, which fixes $1, 4, 7$ and interchanges 2 with 5 and 3 with 6. Then deleting the parentheses, we have a listing of the elements of $\{1, 2, \cdots, n\}$ in some order, which we can interpret as $\sigma'(1)\sigma'(2)\cdots\sigma'(n)$ for some permutation $\sigma'$. In our example, $\sigma'$ sends 1 to 7, 2 to 4, 3 to 3, 4 to 6, 5 to 2, 6 to 5 and 7 to 1. It is easy to see that $\sigma'$ is always modest: if $\sigma'(i)$ is the smaller element of a 2-cycle of $\sigma$ then $\sigma'(i+2)$ is the smaller element of the next cycle, so by our choice of ordering we have $\sigma'(i) > \sigma'(i+2)$; and similarly, if $\sigma'(i)$ is a 1-cycle or the larger element of a 2-cycle of $\sigma$ then we have $\sigma'(i) > \sigma'(i+1)$. To show that this map $\sigma \mapsto \sigma'$ is a bijection from self-inverse to modest permutations, we must show that, given a modest permutation $\sigma'$ written out as $\sigma'(1)\sigma'(2)\cdots\sigma'(n)$, there is a unique way to insert parentheses to break it into 1-cycles and 2-cycles that satisfy the ordering convention. This is also easy: work from left to right, and make a 2-cycle whenever there is an ascent from one place to the next.

**6.** Let $f(x)$ be a polynomial function with rational coefficients and degree at least 2. Show that there are infinitely many rational numbers that are not equal to $f(x)$ for any rational $x$.

**Solution.** Multiplying $f$ by a nonzero rational scalar or adding to $f$ a rational constant doesn't affect the property we need to prove, so we can assume that $f$ has integer coefficients, positive leading coefficient and zero constant term. Thus

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x$$

for some integers $d \geq 2$ and $a_1, \cdots, a_d$, with $a_d > 0$. We will then show that there are infinitely many integers that are not equal to $f(x)$ for any rational $x$.

If $d$ is even, then as a function of a real variable, $f(x) \to \infty$ as $x \to \pm\infty$, so $f(x)$ attains some global minimum value $M$. The claim is then obvious because there are infinitely many integers less than $M$. So we could assume that $d$ is odd, but it makes no difference to the following argument whether we do or not.

Since $d \geq 2$, we have $f(x) \to \infty$ as $x \to \infty$ and also $f'(x) \to \infty$ as $x \to \infty$. There is then some $N > 0$ such that:

a) $f(x) \geq f(N) \Rightarrow x \geq N$;

b) $x \geq N \Rightarrow f'(x) > a_d$ (in particular, $f$ is increasing on $[N, \infty)$).

If $f(q) = t$ is an integer for some rational $q = \frac{r}{s}$, where $r, s$ are integers with $\gcd(r, s) = 1$, then by the rational roots theorem we have $s \mid a_d$, so $q \in \frac{1}{a_d}\mathbb{Z}$. If the integer $t$ also satisfies $t \geq f(N)$, we have $q \geq N$ by property (1), so $f'(x) > a_d$ for all $x$ in the interval $[q, q + \frac{1}{a_d}]$ by property (2), so $f(q + \frac{1}{a_d}) > t + 1$, so $t + 1$ is not of the form $f(q')$ for any rational $q'$. In other words, no two consecutive integers $\geq f(N)$ can both be of the form $f(q)$ for $q$ rational; clearly this means that there are infinitely many integers not of this form.

With a bit more work, one can show that the set of rational numbers that are not equal to $f(x)$ for any rational $x$ is not just infinite but dense.

**7.** For any positive integer $n$, let $A_n$ be the $2 \times 2$ matrix $\begin{bmatrix} \frac{n}{n+1} & 2 \\ \frac{2n}{n+1} & 1 \end{bmatrix}$. Define $B_n = A_1 A_2 \cdots A_n$. Show that the entries in the bottom row of $B_n$ are integers.

**Solution.** Let $c_n, d_n$ be the entries in the bottom row of $B_n$, so $B_n = \begin{bmatrix} ? & ? \\ c_n & d_n \end{bmatrix}$. By definition, the sequences $c_n, d_n$ are determined by the initial conditions

$$c_0 = 0, \ d_0 = 1,$$

and the following recurrence relations for $n \geq 1$:

$$\begin{aligned} c_n &= (\frac{n}{n+1})c_{n-1} + (\frac{2n}{n+1})d_{n-1}, \\ d_n &= 2c_{n-1} + d_{n-1}. \end{aligned}$$

Now let $C_n$ and $D_n$ be the coefficients of $x^{n+1}$ and $x^n$ respectively in $(x^2+x+1)^n$. Obviously $C_n$ and $D_n$ are integers (one could give formulas for them as sums of multinomial coefficients, but this is unnecessary for the present argument). We claim that in fact $c_n = C_n$ and $d_n = D_n$, which solves the problem. To show this, it suffices to show that $C_n, D_n$ satisfy the same initial conditions and recurrence relations as $c_n, d_n$. The initial conditions $C_0 = 0, D_0 = 1$ are obvious.

For $n \geq 1$, consider the coefficient of $x^n$ in $\dfrac{d}{dx}(x^2+x+1)^n$. On the one hand, it is $(n+1)C_n$. On the other hand, it is the coefficient of $x^n$ in $n(2x+1)(x^2+x+1)^{n-1}$, which is $2nD_{n-1} + nC_{n-1}$. So $(n+1)C_n = 2nD_{n-1} + nC_{n-1}$, which rearranges to the first recurrence relation.

From $(x^2+x+1)^n = (x^2+x+1)(x^2+x+1)^{n-1}$, we see that $D_n$ is the sum of the coefficients of $x^{n-2}$, $x^{n-1}$, and $x^n$ in $(x^2+x+1)^{n-1}$. But the coefficients of $(x^2+x+1)^{n-1}$ are obviously symmetric about the middle $x^{n-1}$ term, so the coefficient of $x^{n-2}$ equals the coefficient of $x^n$. Thus $D_n = 2C_{n-1} + D_{n-1}$, the second desired recurrence relation.

**8.** Let $a$ and $c$ be positive real numbers. Evaluate

$$\int_{c-i\infty}^{c+i\infty} \frac{a^z}{z^2}\, dz.$$

Here $\int_{c-i\infty}^{c+i\infty}$ denotes a contour integral in the complex plane, along the vertical line $\mathrm{Re}\,(z) = c$ traversed upwards.

**Solution.** Let $f(z) = \frac{a^z}{z^2}$. Note that $f$ is defined on the whole complex plane except at $0$, where it has a pole of order $2$ with residue

$$\mathrm{Res}(f,0) = \lim_{z\to 0} \frac{d}{dz}(z^2 f(z)) = \lim_{z\to 0} \frac{d}{dz}(a^z) = \lim_{z\to 0} a^z \log a = \log a.$$

The answer to the question is that

$$\int_{c-i\infty}^{c+i\infty} f(z)\, dz = \begin{cases} 2\pi i \log a & \text{if } a > 1, \\ 0 & \text{if } 0 < a \leq 1. \end{cases}$$

First consider the case where $a > 1$. Fix $R > c$. Let $\gamma_R$ denote the left semicircle centred at $c$ with radius $R$, parametrized by $\gamma_R(t) = c + Re^{it}$ with $t \in [\pi/2, 3\pi/2]$. Let $L_R$ be the line segment from $c - iR$ to $c + iR$. For $z \in \gamma_R$, we have $\mathrm{Re}\,(z) \leq c$ and $|z|^2 \geq (R-c)^2$ so that $|a^z| = a^{\mathrm{Re}\, z} \leq a^c$ and $|z|^{-2} \leq (R-c)^{-2}$. It follows that

$$\left| \int_{\gamma_R} \frac{a^z}{z^2}\, dz \right| \leq \int_{\gamma_R} a^c (R-c)^{-2}\, dz = a^c (R-c)^{-2} \pi R \to 0 \text{ as } R \to \infty.$$

Therefore, $\int_{\gamma_R} f(z)\, dz \to 0$ as $R \to \infty$. On the other hand, the Residue Theorem applied to $f$ on the contour $L_R \cup \gamma_R$ says that

$$\int_{\gamma_R} f(z)\, dz + \int_{c-iR}^{c+iR} f(z)\, dz = 2\pi i\, \mathrm{Res}\,(f,0) = 2\pi i \log a.$$

By taking $R \to \infty$, we obtain that $\int_{c-i\infty}^{c+i\infty} f(z)\, dz = 2\pi i \log a$.

Next consider the case where $a \leq 1$. Again fix $R > c$. Now let $\tilde{\gamma}_R$ denote the right semicircle centred at $c$ with radius $R$, parametrized by $\tilde{\gamma}_R(t) = c + Re^{it}$ with $t \in [-\pi/2, \pi/2]$. Let $\tilde{L}_R$ be the line segment from $c + iR$ to $c - iR$. For $z \in \tilde{\gamma}_R$, we have $\mathrm{Re}\, z \geq c$ and $|z|^2 \geq R^2 + c^2$ so that $|a^z| = a^{\mathrm{Re}\, z} \leq a^c$ (since $0 < a \leq 1$) and $|z|^{-2} \leq (R^2 + c^2)^{-1}$. It follows that

$$\left| \int_{\gamma_R} \frac{a^z}{z^2}\, dz \right| \leq \int_{\gamma_R} a^c (R^2+c^2)^{-1}\, dz = a^c (R^2+c^2)^{-1} \pi R \to 0 \text{ as } R \to \infty.$$

Hence, as before, $\int_{\gamma_R} f(z)\,dz \to 0$ as $R \to \infty$. Inside the contour $\tilde{L}_R \cup \tilde{\gamma}_R$, $f$ has no pole. By Cauchy's Theorem, we have

$$\int_{\tilde{\gamma}_R} f(z)\,dz - \int_{c-iR}^{c+iR} f(z)\,dz = 0.$$

Taking $R \to \infty$, we conclude that $\int_{c-i\infty}^{c+i\infty} f(z)\,dz = 0$.

**9.** Let $\mathbb{N} = \{0, 1, 2, \cdots\}$. Call a subset $A \subseteq \mathbb{N}$ *special* if it satisfies:

a) $0 \in A$,

b) $a \in A \Rightarrow a + 10 \in A$,

c) $a \in A \Rightarrow a + 2013 \in A$.

How many special subsets $A \subseteq \mathbb{N}$ are there?

**Solution.** Replace the numbers 10 and 2013 with the general positive integers $p$ and $q$ respectively. As long as $p$ and $q$ are coprime (which 10 and 2013 certainly are), we claim that the number of special subsets is $\frac{1}{p+q}\binom{p+q}{p}$. So the answer to the original question is $\frac{1}{2023}\binom{2023}{10}$.

Firstly, it is a standard fact that every integer $N > pq - p - q$ can be written as $ap + bq$ for some $a, b \in \mathbb{N}$. The proof of this is as follows. By elementary number theory we can write $N$ as $a'p + b'q$ for some $a', b' \in \mathbb{Z}$, and clearly one of $a', b'$ must be positive. Without loss of generality, assume that $a' > 0$ and write $a' = mq + a$ where $m \in \mathbb{N}$ and $0 \leq a \leq q - 1$. Set $b = b' + mp$. Then $N = ap + bq$, and we cannot have $b \leq -1$ since this would imply $N \leq (q-1)p - q$, contrary to assumption.

From the definition it is obvious that a special subset of $\mathbb{N}$ must contain every integer of the form $ap + bq$ for $a, b \in \mathbb{N}$. Consequently, a special subset must contain all the integers greater than $pq - p - q$. This already shows that the number of special subsets is finite.

If $A$ is a special subset, say that an element $i \in A$ is *basic* if $i - p - q \notin A$. For example, the element 0 is guaranteed to be basic. Note that $i \in A \Rightarrow i + k(p+q) \in A$ for all $k \in \mathbb{N}$, so $i$ is basic if and only if it is the smallest element in its congruence class modulo $p + q$ to belong to $A$. Since $A$ contains representatives of each congruence class modulo $p+q$, $A$ contains exactly $p + q$ basic elements. Note that the set of basic elements of $A$ determines the whole of $A$.

Let $X$ be the set of pairs $(A, i)$ where $A$ is a special subset of $\mathbb{N}$ and $i \in A$ is basic. It suffices to show that $|X| = \binom{p+q}{p}$. To do this, we construct a bijection between $X$ and a set $Y$ whose cardinality is obviously $\binom{p+q}{p}$, namely the set of $(p+q)$-tuples $(a_1, a_2, \cdots, a_{p+q})$ where $a_i \in \{-p, q\}$ for all $i$, and $a_i = -p$ for exactly $q$ values of $i$.

The map $f : X \to Y$ is defined as follows. If $j$ is basic in a special subset $A$, then there is a unique basic element $k$ of $A$ congruent to $j + q$ modulo $p + q$. Since $j + q \in A$, we certainly have $k \leq j + q$. But also $j - 2p - q \notin A$ (or else $j - p - q \in A$ contrary to assumption), so $k \geq j - p$. We conclude that $k$ is either $j - p$ or $j + q$. Now given $(A, i) \in X$, we can define $f(A, i) = (a_1, a_2, \cdots, a_{p+q})$ by the rule that $i + a_1$ is the basic element of $A$ congruent to $i + q$, $i + a_1 + a_2$ is the basic element of $A$ congruent to $i + 2q$, and so on, including the stipulation that $i + a_1 + \cdots + a_{p+q}$ is the basic element of $A$ congruent to $i$, which is equivalent to saying that $a_1 + \cdots + a_{p+q} = 0$. By what we have seen, each $a_i$ equals either $-p$ or $q$. If $s$ of the $a_i$'s equal $-p$, then we must have $s(-p) + (p+q-s)q = 0$, which forces $s = uq$ and $p + q - s = up$ for some $u \in \mathbb{Z}$ (since $p$ and $q$ are coprime), leading to $u = 1$ and $s = q$. So $(a_1, a_2, \cdots, a_{p+q})$ does indeed belong to $Y$.

The inverse map $g : Y \to X$ is defined as follows. Given $(a_1, a_2, \cdots, a_{p+q}) \in Y$, consider the set $B$ of partial sums $\{0, a_1, a_1 + a_2, \cdots, a_1 + \cdots + a_{p+q-1}\}$. Each congruence class modulo

$p+q$ is represented exactly once in $B$, for if there were two different elements of $B$ congruent modulo $p+q$, then we would have $s(-p)+tq = u(p+q)$ for some $s,t \in \mathbb{N}$ and $u \in \mathbb{Z}$ with $0 < s+t < p+q$, leading to $s+u = vq$, $t-u = vp$ for some $v \in \mathbb{Z}$ and then a contradiction. Let $b = \min B$ (a nonpositive integer) and translate to obtain a subset $B-b \subseteq \mathbb{N}$ with minimum element $0$, in which each congruence class modulo $p+q$ is represented exactly once. Let $A$ be the union of the sets $j+\mathbb{N}(p+q)$ as $j$ runs over $B-b$. We claim that $A$ is special. To prove this claim, it suffices to show that $j+p, j+q \in A$ for any $j \in B-b$. But by definition of $B$, if $j+b \in B$ then either $j+b+p$ or $j+b-q$ belongs to $B$ (this is $a_1+\cdots+a_{i-1}$ where $j+b = a_1+\cdots+a_i$ for $1 \le i \le p+q$) and also either $j+b-p$ or $j+b+q$ belongs to $B$ (this is $a_1+\cdots+a_i$ where $j+b = a_1+\cdots+a_{i-1}$ for $1 \le i \le p+q$), so our claim follows. Note that the set of basic elements of $A$ is exactly $B-b$. Hence we can define $g(a_1,a_2,\cdots,a_{p+q})$ to be the pair $(A,i)$ where $A$ is as above and $i=-b$.

It is easy to check that $g \circ f$ is the identity on $X$: for $(A,i) \in X$, if we define $(a_1,a_2,\cdots,a_{p+q})$ as in the definition of $f$, then $B+i$ is the set of basic elements of $A$, so $\min B = -i$ and $g(a_1,a_2,\cdots,a_{p+q}) = (A,i)$. It is also easy to check that $f \circ g$ is the identity on $Y$: for $(a_1,a_2,\cdots,a_{p+q}) \in Y$, if we define $(A,i)$ as in the definition of $g$, then the set of basic elements of $A$ is $B+i = \{i, i+a_1, i+a_1+a_2, \cdots\}$, which implies that $f(A,i) = (a_1,a_2,\cdots,a_{p+q})$. The proof is finished.

**10.** Let $A,B,C,D$ be matrices over the complex numbers satisfying the following conditions:

a) $A,B$ are $n \times n$ matrices that are *nilpotent* (so $A^n = B^n$ is the zero matrix);

b) $C$ is an $n \times 2$ matrix and $D$ is a $2 \times n$ matrix;

c) $A+B = CD$.

Show that $DA^iC + (-1)^{i+1}DB^iC$ is a scalar matrix for all nonnegative integers $i$.

**Solution.** It is convenient to work in the ring $\mathrm{Mat}_2(\mathbb{C}[z])$ of $2\times 2$ matrices whose entries are polynomials in the variable $z$. We define two elements of this ring:

$$F(z) = I + \sum_{i\ge 0} DA^iC\, z^{i+1},$$
$$G(z) = I + \sum_{i\ge 0} (-1)^{i+1} DB^iC\, z^{i+1}.$$

The entries are indeed polynomials because $A$ and $B$ are nilpotent, so all terms with $i \ge n$ vanish. Observe that

$$\begin{aligned}
F(z)G(z) &= I + \sum_{j\ge 0}\left((-1)^{j+1}DB^jC + \sum_{i=0}^{j-1}(-1)^{j-i}DA^iCDB^{j-i-1}C + DA^jC\right)z^{j+1}\\
&= I + \sum_{j\ge 0}\left((-1)^{j+1}DB^jC + \sum_{i=0}^{j-1}(-1)^{j-i}DA^i(A+B)B^{j-i-1}C + DA^jC\right)z^{j+1}\\
&= I + \sum_{j\ge 0}\Bigg((-1)^{j+1}DB^jC + \sum_{i=0}^{j-1}(-1)^{j-i}DA^iB^{j-i}C\\
&\qquad + \sum_{i=0}^{j-1}(-1)^{j-i}DA^{i+1}B^{j-i-1}C + DA^jC\Bigg)z^{j+1}\\
&= I \text{ (by pairwise cancellation of terms).}
\end{aligned}$$

Now elements of $\mathrm{Mat}_2(\mathbb{C}[z])$ have determinants, defined in the usual way, which are polynomials in $z$. The fact that $F(z)G(z) = I$ implies as usual that $\det(F(z))\det(G(z)) = 1$ (the constant polynomial). If the product of two polynomials is $1$, they must be constant; since the constant term of $\det(F(z))$ is $\det(F(0)) = 1$, we conclude that $\det(F(z)) = \det(G(z)) = 1$.

We have the usual formula for the inverse of a $2 \times 2$ matrix with determinant $1$, showing that if $H(z) \in \mathrm{Mat}_2(\mathbb{C}[z])$ has $\det(H(z)) = 1$, then $H(z) + H(z)^{-1}$ is a scalar matrix (off-diagonal entries zero, diagonal entries equal). So $F(z)+G(z)$ is a scalar matrix. Extracting the coefficient of $z^{i+1}$, this means that $DA^iC + (-1)^{i+1}DB^iC$ is a scalar matrix for all $i \geq 0$, as required.

The argument also shows something about traces: if $H(z) \in \mathrm{Mat}_2(\mathbb{C}[z])$ has $\det(H(z)) = 1$, then $\mathrm{tr}(H(z)^{-1}) = \mathrm{tr}(H(z))$, so we can conclude that $\mathrm{tr}(DA^iC) = \mathrm{tr}((-1)^{i+1}DB^iC)$.