SUMS PROBLEM COMPETITION, 2001

SOLUTIONS

1. Suppose that after n visits to Aunt Joylene (and therefore also n visits to Uncle Bruce) Linda has t_n ten cent pieces and d_n dollar coins. After a visit to Uncle Bruce she has $2d_n$ twenty cent pieces and $t_n + d_n$ fifty cent pieces. So after her next visit to Aunt Joylene she has $2(t_n + d_n)$ ten cent pieces and $2d_n + (t_n + d_n)$ dollar coins. Thus

$$\begin{aligned} t_{n+1} &= 2t_n + 2d_n \\ d_{n+1} &= t_n + 3d_n. \end{aligned}$$

Hence

$$\begin{aligned} t_{n+2} &= 2t_{n+1} + 2d_{n+1} \\ &= 2t_{n+1} + 2(t_n + 3d_n) \\ &= 2t_{n+1} + 2t_n + 3(t_{n+1} - 2t_n), \end{aligned}$$

so that

$$t_{n+2} - 5t_{n+1} + 4t_n = 0. \tag{1}$$

This is a second order linear recurrence equation with constant coefficients. The solution is found by first solving the auxiliary equation $\lambda^2 - 5\lambda + 4 = 0$. The roots are $\lambda_1 = 4$ and $\lambda_2 = 1$. Then the general solution to the recurrence relation (1) is

$$A\lambda_1^n + B\lambda_2^n = A\,4^n + B. \tag{2}$$

We are told that $t_0 = 0$ and that $d_0 = 1$. Hence $t_1 = 2t_0 + 2d_0 = 2$. Using $t_0 = 0$ and $t_1 = 2$, we quickly find that the constants A and B are $2/3$ and $-2/3$, respectively. So

$$t_n = \left(\frac{2}{3}\right)4^n - \frac{2}{3}.$$

Similarly, the d_n satisfy the recurrence relation $d_{n+2} - 5d_{n+1} + 4d_n = 0$, and d_n is given by a formula (2). Since $d_0 = 1$ and $d_1 = t_0 + 3d_0 = 3$, we quickly find that $A = 2/3$ and $B = 1/3$ this time. Hence

$$d_n = \left(\frac{2}{3}\right)4^n + \frac{1}{3}.$$

Hence after n visits to Aunt Joylene, Linda has

$$d_n + \frac{1}{10}t_n = \left(\frac{11}{15}\right)4^n + \frac{4}{15} \quad \text{dollars.}$$

2. We consider more generally the case of $n \geq 3$ delegates sitting around a round table, each putting their document on their own seat and that of their two immediate neighbours. There are 3^n different ways for the thief to steal the documents, corresponding to the three choices he has at each seat. So the probability of obtaining a complete set is $N_n/3^n$, where N_n is the number of ways of stealing them which result in a complete set.

We shall show that $N_n = F_{n+1} + F_{n-1} + 2$, where F_n is the n-th Fibonacci number, defined by $F_1 = 1$, $F_2 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 1$, so that $F_3 = 2$, $F_4 = 3$, etc.

In the particular case $n = 12$ this gives $N_{12} = F_{13} + F_{11} + 2 = 233 + 89 + 2 = 324$, so that the probability of getting a complete set is

$$\frac{324}{3^12} = \frac{4}{3^8} = \frac{4}{6561}.$$

Let us label the seats $0, \ldots, n-1$. Then on seat i, we have documents $i-1$, i and $i+1$, these expressions being understood modulo n. Thus in front of seat 0 we have documents n, 0 and 1; in front of seat 1 we have documents 0, 1 and 2, etc, until in front of seat $n-1$ we have documents $n-2$, $n-1$ and 0.

The key to deriving the above formula for N_n is the following observation:

Suppose that the thief takes document $i-1$ from seat i *and* he takes document i from seat $i+1$. Then he must take document $i+1$ from seat $i+2$, since otherwise he would miss that document. Continuing clockwise around the table, we see that he must take document $j-1$ from seat j for *every* j.

Seat number :	$\cdots$	$i-1$	i	$i+1$	$i+2$	$\cdots$
	$\cdots$	$i-2$	$i-1$	i	$i+1$	$\cdots$
	$\cdots$	$i-1$	i	$i+1$	$i+2$	$\cdots$
	$\cdots$	i	$i+1$	$i+2$	$i+3$	$\cdots$

Similarly, if the thief takes document $i+1$ from seat i *and* he takes document $i+2$ from seat $i+1$. Then he must take document i from seat $i-1$. Continuing anti-clockwise around the table, we see that he must take document $j+1$ from seat j for *every* j.

If the thief takes document $j-1$ from seat j for every j, or if he takes document $j+1$ from seat j for every j, then we shall say that he has committed a *special* theft.

When a thief steals the documents, let us write $f(i) = j$ if he steals document j from seat i. Then

$$f : \{0, \ldots, n-1\} \to \{0, \ldots, n-1\} \tag{1}$$

is a function. To say that he gets a complete set is to say that f is surjective. Since the domain and codomain are of the same size, this is equivalent to f being injective, or to f being a bijection. So the number N_n is the number of bijections (1) such that $f(i) \in \{i-1, i, i+1\}$ for all i. We call the bijections $f(i) \equiv i-1$ and $f(i) \equiv i+1$ *special.*

Let N'_n denote the number of non-special bijections (1) such that $f(i) \in \{i-1, i, i+1\}$ for all i. Given such a bijection, let

$$S_f = \{i \in \{0, \ldots, n-1\} : f(i) = i+1\}.$$

If $i \in S_f$, then $f(i+1)$ cannot equal $i+1$ since f is injective, and it cannot equal $i+2$, since otherwise f would be special by the key observation above. Hence $f(i+1)$ must be i. In particular, $i+1 \notin S_f$. For the same reasons, if $i-1 \in S_f$, then $f(i)$ must be $i-1$.

If neither i nor $i-1$ is in S_f, then $f(i)$ must be i. For $f(i) = i-1$ would imply that $f(i+1) \neq i$ by the above key observation, and so $i-1 \notin S_f$, i.e., $f(i-1) \neq i$, then implies that document i would be missed.

Conversely, suppose that $S \subset \{0, \ldots, n-1\}$ has the property that

$$i \in S \Rightarrow i+1 \notin S. \tag{2}$$

Define $f_S : \{0,\dots,n-1\} \to \{0,\dots,n-1\}$ by setting

$$f_S(i) = \begin{cases} i+1 & \text{if } i \in S, \\ i-1 & \text{if } i-1 \in S, \\ i & \text{if } i, i-1 \notin S. \end{cases}$$

Then $f = f_S$ is a non-special bijection (1), and $S = \{i : f_S(i) = i+1\}$. This shows that the set of non-special bijections (1) are in one to one correspondence with the set of subsets $S \subset \{0,\dots,n-1\}$ having property (2). Hence N'_n is the number of such subsets.

Another way of expressing property (2) is to say that S contains none of the subsets $\{0,1\}, \{1,2\}, \dots, \{n-2, n-1\}, \{n-1, 0\}$.

To evaluate N'_n, it is convenient to express N'_n in terms of the number A_m of subsets S of $\{1,\dots,m\}$ such that

$$i \in S \Rightarrow i+1 \notin S \quad \text{for } i = 1,\dots,m-1. \tag{3_m}$$

Note that we are not using arithmetic modulo n (or modulo m) here. Let us show that $A_m = A_{m-1} + A_{m-2}$ for all $m \geq 3$. For let S be a subset of $\{1,\dots,m\}$ satisfying (3_m). If $m \in S$, then $m-1$ cannot be in S, and so $S = S' \cup \{m\}$, where $S' \subset \{1,\dots,m-2\}$ satisfies (3_{m-2}). On the other hand, if $m \notin S$, then S is a subset of $\{1,\dots,m-1\}$ satisfying (3_{m-1}). The set of subsets S of $\{1,\dots,m\}$ satisfying (3_m) is therefore the union of two disjoint subsets, one with A_{m-2} elements, the other with A_{m-1}. Hence $A_m = A_{m-1} + A_{m-2}$ for all $m \geq 3$.

Notice that $A_1 = 2 = F_3$ (the subsets being $\emptyset$ and $\{0\}$) and $A_2 = 3 = F_4$ (the subsets being $\emptyset$, $\{0\}$ and $\{1\}$). It follows by induction that $A_m = F_{m+2}$ for $m = 1, 2, \dots$.

We now relate the numbers A_m to what we really want: N'_n. If $S \subset \{0,\dots,n-1\}$ has the property (2) (which is understood using arithmetic modulo n), then either $n-1 \in S$ or $n-1 \notin S$. If $n-1 \in S$, then $0 \notin S$ and also $n-2 \notin S$. Hence $S' = S \setminus \{n-1\}$ must be a subset of $\{1,\dots,n-3\}$, and it must satisfy (3_{n-3}). There are $A_{n-3} = F_{n-1}$ such subsets. If $n-1 \notin S$, then S is a subset of $\{0,\dots,n-2\}$ so that $S+1 = \{i+1 : i \in S\}$ is a subset of $\{1,\dots,n-1\}$ satisfying (3_{n-1}). There are $A_{n-1} = F_{n+1}$ such subsets. The set of subsets S of $\{0,\dots,n-1\}$ satisfying (2) is therefore the union of two disjoint subsets, one with F_{n-1} elements, the other with F_{n+1}. Hence $N'_n = F_{n+1} + F_{n-1}$ for all $n \geq 2$. Thus $N_n = N'_n + 2 = F_{n+1} + F_{n-1} + 2$. for all $n \geq 2$.

3. *Solution 1.* We may assume our space has coordinate axes so that the origin is one corner of the larger box B', and that B' lies in the first octant. Hence B' is bounded by the 6 planes $x = 0$, $x = \ell'$, $y = 0$, $y = h'$, $z = 0$ and $z = b'$. Now suppose that P is one corner of the smaller box, with coordinate vector $\mathbf{p} = (p_x, p_y, p_z)$. Let $\mathbf{p} + \mathbf{u}$, $\mathbf{p} + \mathbf{v}$ and $\mathbf{p} + \mathbf{w}$ be the coordinate vectors of the vertices of B which are joined by an edge to P. Suppose that $\mathbf{u}$ has coordinates (u_x, u_y, u_z), and similarly for $\mathbf{v}$ and $\mathbf{w}$. Notice that some or all of u_x, u_y and u_z might be negative (several entries were not correct because they didn't consider this possibility). The length, breadth and height of B are the lengths of the vectors $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$ (in that order, say):

$$\ell = \|\mathbf{u}\| = \sqrt{u_x^2 + u_y^2 + u_z^2}, \; b = \|\mathbf{v}\| = \sqrt{v_x^2 + v_y^2 + v_z^2} \quad \text{and} \quad h = \|\mathbf{w}\| = \sqrt{w_x^2 + w_y^2 + w_z^2}$$

By the triangle inequality,

$$\begin{aligned} \ell = \|\mathbf{u}\| = \|(u_x,0,0) + (0,u_y,0) + (0,0,u_z)\| &\leq \|(u_x,0,0)\| + \|(0,u_y,0)\| + \|(0,0,u_z)\| \\ &= |u_x| + |u_y| + |u_z|. \end{aligned}$$

Similarly,

$$b \le |v_x| + |v_y| + |v_z| \quad \text{and} \quad h \le |w_x| + |w_y| + |w_z|.$$

The four vertices of B which are not joined by an edge to P have coordinate vectors $\mathbf{p}+\mathbf{u}+\mathbf{v}$, $\mathbf{p}+\mathbf{u}+\mathbf{w}$, $\mathbf{p}+\mathbf{v}+\mathbf{w}$ and $\mathbf{p}+\mathbf{u}+\mathbf{v}+\mathbf{w}$.

Let us show that

$$|u_x| + |v_x| + |w_x| \le \ell'. \tag{1}$$

To see this, project the 8 vertices of B onto the x-axis. In other words, look at the eight numbers

$$\begin{aligned} &p_x,\ p_x+u_x,\ p_x+v_x,\ p_x+w_x,\\ &p_x+u_x+v_x,\ p_x+u_x+w_x,\ p_x+v_x+w_x,\ p_x+u_x+v_x+w_x. \end{aligned}$$

These must all be between 0 and ℓ', because $B \subset B'$ implies that all points of B are between the two planes $x = 0$ and $x = \ell'$. So the difference between any two of them must be in modulus at most ℓ'. For example,

$$|(p_x + u_x + v_x) - (p_x + w_x)| = |u_x + v_x - w_x|$$

must be at most ℓ'. There are 8 possible choices of the signs of u_x, v_x and w_x. If all are ≥ 0 or all are ≤ 0, then (1) holds because

$$|u_x| + |v_x| + |w_x| = |u_x + v_x + w_x| = |(p_x + u_x + v_x + w_x) - p_x| \le \ell'.$$

If two of u_x, v_x and w_x are ≥ 0 and one is ≤ 0, say $u_x, v_x \ge 0$ and $w_x \le 0$, then (1) holds because

$$|u_x| + |v_x| + |w_x| = u_x + v_x + (-w_x) \le |u_x + v_x - w_x| = |(p_x + u_x + v_x) - (p_x + w_x)| \le \ell',$$

as observed above. Similarly if one of u_x, u_y and u_z is ≥ 0 and two are ≤ 0, then (1) holds.

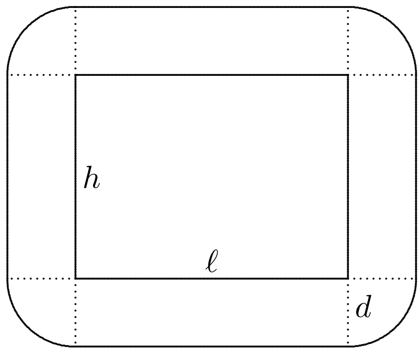
Similarly, we have

$$|u_y| + |v_y| + |w_y| \le b' \quad \text{and} \quad |u_z| + |v_z| + |w_z| \le h'.$$

Hence

$$\begin{aligned} \ell + b + h &\le (|u_x| + |u_y| + |u_z|) + (|v_x| + |v_y| + |v_z|) + (|w_x| + |w_y| + |w_z|)\\ &= (|u_x| + |v_x| + |w_x|) + (|u_y| + |v_y| + |w_y|) + (|u_z| + |v_z| + |w_z|)\\ &\le \ell' + b' + h'. \end{aligned}$$

Solution 2. The idea is to take neighbourhoods of both boxes. Let B_d denote the set of points which are at distance at most d from a point in B, and similarly for B'. We compare $\mathrm{vol}(B_d)$ and $\mathrm{vol}(B'_d)$. Let us illustrate the idea in 2 dimensions first, where we compare areas.



B_d

The area of B_d is easily seen to be

$$\ell h + 2(\ell + h)d + \pi d^2.$$

Since $B \subset B'$, we have $B_d \subset B'_d$ for every d, and so

$$\ell h + 2(\ell + h)d + \pi d^2 \leq \ell' h' + 2(\ell' + h')d + \pi d^2.$$

Subtracting πd^2 from both sides and dividing by $2d$, we have

$$\frac{\ell h}{2d} + \ell + h \leq \frac{\ell' h'}{2d} + \ell' + h'.$$

This is true for every $d > 0$. Now let $d \to \infty$, and we get $\ell + h \leq \ell' + h'$.

The proof in 3 dimensions is similar. One can easily show that

$$\mathrm{vol}(B_d) = \ell bh + 2(\ell b + \ell h + bh)d + (\ell + b + h)\pi d^2 + \frac{4}{3}\pi d^3.$$

From $\mathrm{vol}(B_d) \leq \mathrm{vol}(B'_d)$ we see that

$$\ell bh + 2(\ell b + \ell h + bh)d + (\ell + b + h)\pi d^2 \leq \ell' b' h' + 2(\ell' b' + \ell' h' + b' h')d + (\ell' + b' + h')\pi d^2.$$

Dividing by πd^2 and letting d tend to infinity, we find that $\ell + b + h \leq \ell' + b' + h'$.

4. There were several correct solutions to the first part of the question. For the second part, the equation $4n(n+1)\alpha(n)^2 + 1 = x^2$ can be written $x^2 - n(n+1)y^2 = 1$ for $y = 2\alpha(n)$, and so is an example of Pell's equation, which is treated in many books using continued fractions, etc, and this approach was followed successfully by some entrants. We give instead the following elementary solution (submitted by Van Minh Nguyen), and his solution to the first part using similar methods.

Suppose that $4n(n+1)a^2 + 1$ is a perfect square for $n = 0, 1, \ldots$. Of course $a = 0$ has this property, and so we assume that $a \geq 1$. Write $4n(n+1)a^2 + 1 = m_n^2$, where $m_n \geq 0$ is an integer. Using $a \leq a^2$ and $1 \leq a^2$, we get

$$(2na+1)^2 = 4n^2a^2 + 4na + 1 \leq 4n^2a^2 + 4na^2 + 1 = m_n^2 \leq 4n(n+1)a^2 + a^2 = ((2n+1)a)^2, \quad (1)$$

and so $2na+1 \leq m_n \leq (2n+1)a$. So we may write $m_n = 2na + x_n$, where $1 \leq x_n \leq a$ for all n. Hence

$$4n(n+1)a^2 + 1 = (2na + x_n)^2, \tag{2}$$

so that

$$x_n = a + \frac{1}{4an} - \frac{x_n^2}{4an} \to a \quad \text{as } n \to \infty$$

(we use $1 \leq x_n \leq a$ to see that $x_n^2/4an \leq a^2/4an = a/4n$ here). But x_n is an integer, and so $x_n = a$ must hold if n is sufficiently large. For such n, (2) tells us that

$$4n(n+1)a^2 + 1 = (2na + a)^2,$$

from which we see that $a = 1$.

Now suppose that $\alpha(n) = an + b$ has the property that $4n(n+1)\alpha(n)^2 + 1$ is a perfect square for $n = 0, 1, \ldots$. Again write $4n(n+1)\alpha(n)^2 + 1 = m_n^2$, where $m_n \geq 0$ is an integer. There were several incomplete solutions to this part of the problem, in which, without justification, it was assumed that $m_n = cn^2 + dn + e$ for some constants c, d and e. The proof below essentially provides the justification for this.

If $a = 0$, then $b = 1$ by the first part, and so assume that $a \geq 1$. Then $\alpha(n) \geq 1$ for all $n \geq 1$, and so, replacing a by $\alpha(n)$ in (1) above,

$$(2n\alpha(n) + 1)^2 \leq m_n^2 \leq ((2n+1)\alpha(n))^2$$

so that $m_n = 2n\alpha(n) + x_n$, where $1 \leq x_n \leq \alpha(n)$. Replacing a by $\alpha(n)$ in (2), we get

$$4n(n+1)\alpha(n)^2 + 1 = (2n\alpha(n) + x_n)^2, \tag{3}$$

Therefore

$$x_n = \alpha(n) + \frac{1}{4\alpha(n)n} - \frac{x_n^2}{4\alpha(n)n},$$

and so

$$\frac{x_n}{n} = \frac{\alpha(n)}{n} + \frac{1}{4\alpha(n)n^2} - \frac{x_n^2}{4\alpha(n)n^2} \to a \quad \text{as } n \to \infty$$

(we use $1 \leq x_n \leq \alpha(n)$ to see that $x_n^2/4\alpha(n)n^2 \leq \alpha(n)/4n^2 \to 0$ here). So we can write $x_n = an + y_n$, where $y_n/n \to 0$ as $n \to \infty$. Substituting this into (3), we get

$$4n(n+1)\alpha(n)^2 + 1 = (2n\alpha(n) + an + y_n)^2,$$

and so

$$y_n = \frac{4b-a}{4} - \frac{y_n}{2n} + \frac{b^2}{an} - \frac{by_n}{an} - \frac{y_n^2}{4an^2} + \frac{1}{4an^2}.$$

This tends to $(4b-a)/4$ as $n \to \infty$. Since y_n is an integer, we must have $y_n = (4b-a)/n$ for sufficiently large n. For such n,

$$4n(n+1)\alpha(n)^2 + 1 = (2n\alpha(n) + an + (4b-a)/4)^2,$$

Expanding both sides, and comparing constant terms and the coefficients of n on both sides, we get

$$8a(a-2b) = 0 \quad \text{and} \quad 16 - a^2 - 8ab - 16b^2 = 0.$$

Since $a > 0$, the first equation tells us that $a = 2b$. Then the second equation becomes $16 - 4b^2 = 0$, so that $b = 2$. Hence $(a, b) = (4, 2)$ is the only solution with $a > 0$. Explicitly,

$$4n(n+1)(4n+2)^2 + 1 = (8n^2 + 8n + 1)^2.$$

5. There were several different solutions to this problem.

Solution 1 (the shortest): Let $A_{m,n} = \frac{(2n)!(2m)!}{n!m!(n+m)!}$. Then it is routine to check that $A_{m,n-1} + A_{m-1,n} = 4A_{m-1,n-1}$. Hence

$$A_{m,n} = -A_{m+1,n-1} + 4A_{m,n-1}.$$

Since $A_{m,0} = \binom{2m}{m}$, the result is now a routine induction on n.

Solution 2: The result is immediate from the following identity (due to Szily, 1895):

$$\frac{(2n)!(2m)!}{n!m!(n+m)!} = \sum_{k=-n}^{n} (-1)^k \binom{2n}{n-k}\binom{2m}{m-k}.$$

This identity is seen by considering $(1-x^2)^n = (1+x)^n(1-x)^n$, using the binomial theorem on the three expressions, and comparing coefficients of x^{2r} on both sides.

Solution 3: For each prime p, let n_p (respectively, d_p) denote the number of times that p divides the numerator (respectively, the denominator) of $\frac{(2n)!(2m)!}{n!m!(n+m)!}$. It is enough to show that $d_p \le n_p$ for each p. Now it is well known that the number of times that p divides $n!$ is

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots,$$

the j-th term of the series being zero if $n < p^j$. So what we need to show is that

$$\sum_{j=1}^{\infty} \left\lfloor \frac{m}{p^j} \right\rfloor + \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor + \sum_{j=1}^{\infty} \left\lfloor \frac{m+n}{p^j} \right\rfloor \le \sum_{j=1}^{\infty} \left\lfloor \frac{2m}{p^j} \right\rfloor + \sum_{j=1}^{\infty} \left\lfloor \frac{2n}{p^j} \right\rfloor,$$

and for this it is sufficient to show that

$$\left\lfloor \frac{m}{p^j} \right\rfloor + \left\lfloor \frac{n}{p^j} \right\rfloor + \left\lfloor \frac{m+n}{p^j} \right\rfloor \le \left\lfloor \frac{2m}{p^j} \right\rfloor + \left\lfloor \frac{2n}{p^j} \right\rfloor$$

for each j. In fact, it is easy to check that

$$\left\lfloor \frac{m}{k} \right\rfloor + \left\lfloor \frac{n}{k} \right\rfloor + \left\lfloor \frac{m+n}{k} \right\rfloor \le \left\lfloor \frac{2m}{k} \right\rfloor + \left\lfloor \frac{2n}{k} \right\rfloor$$

for any integer $k \ge 1$.

6. To sum equals $2 - \log(2\pi)$. To see this, start by writing

$$\sum_{n=2}^{\infty} (-1)^n \frac{n-1}{n(n+1)} \zeta(n) = \sum_{n=2}^{\infty} (-1)^n \frac{n-1}{n(n+1)} \sum_{k=1}^{\infty} \frac{1}{k^n} = \sum_{n=2}^{\infty} \Big(\sum_{k=1}^{\infty} \frac{n-1}{n(n+1)} \Big(\frac{-1}{k} \Big)^n \Big).$$

We next want to interchange the order of this double sum, and write

$$\sum_{n=2}^{\infty}\Big(\sum_{k=1}^{\infty}\frac{n-1}{n(n+1)}\Big(\frac{-1}{k}\Big)^n\Big)=\sum_{k=1}^{\infty}\Big(\sum_{n=2}^{\infty}\frac{n-1}{n(n+1)}\Big(\frac{-1}{k}\Big)^n\Big). \tag{1}$$

The most common theorem allowing us to interchange the order of double sums, and write

$$\sum_{n=1}^{\infty}\Big(\sum_{k=1}^{\infty}a_{n,k}\Big)=\sum_{k=1}^{\infty}\Big(\sum_{n=1}^{\infty}a_{n,k}\Big)$$

has the condition

$$\sum_{n=1}^{\infty}\Big(\sum_{k=1}^{\infty}|a_{n,k}|\Big)<\infty.$$

This condition is not satisfied in the present example, basically because of the first term $1/1^n = 1$ in the series for $\zeta(n)$. So we only look at the series starting at $k = 2$. For all $n \geq 2$, we have the estimate

$$\sum_{k=2}^{\infty}\frac{1}{k^n}\leq\frac{1}{2^n}+\int_2^{\infty}\frac{1}{x^n}\,dx=\frac{1}{2^n}+\frac{1}{n-1}\frac{1}{2^{n-1}}\leq\frac{1}{2^n}+\frac{1}{2^{n-1}}=\frac{3}{2^n},$$

and so it is easy to see that

$$\sum_{n=2}^{\infty}\Big(\sum_{k=2}^{\infty}|a_{n,k}|\Big)<\infty$$

is valid for our $a_{n,k}$'s:

$$a_{n,k}=\frac{n-1}{n(n+1)}\Big(\frac{-1}{k}\Big)^n.$$

Hence for these $a_{n,k}$,

$$\begin{aligned}\sum_{n=2}^{\infty}\Big(\sum_{k=1}^{\infty}a_{n,k}\Big)&=\sum_{n=2}^{\infty}\Big(a_{n,1}+\Big(\sum_{k=2}^{\infty}a_{n,k}\Big)\Big)\\&=\sum_{n=2}^{\infty}a_{n,1}+\sum_{n=2}^{\infty}\Big(\sum_{k=2}^{\infty}a_{n,k}\Big)\\&=\sum_{n=2}^{\infty}a_{n,1}+\sum_{k=2}^{\infty}\Big(\sum_{n=2}^{\infty}a_{n,k}\Big)\\&=\sum_{k=1}^{\infty}\Big(\sum_{n=2}^{\infty}a_{n,k}\Big).\end{aligned}$$

This justifies the interchange of summations in (1). Now the double sum on the right in (1) equals

$$\sum_{k=1}^{\infty}\Big(\sum_{n=2}^{\infty}\Big(\frac{2}{n+1}-\frac{1}{n}\Big)\Big(\frac{-1}{k}\Big)^n\Big).$$

The inner sum can be rewritten

$$(-2k)\sum_{n=1}^{\infty}\frac{1}{n+1}\Big(\frac{-1}{k}\Big)^{n+1}-\sum_{n=1}^{\infty}\frac{1}{n}\Big(\frac{-1}{k}\Big)^{n}. \tag{2}$$

Using

$$\sum_{n=1}^{\infty}\frac{1}{n}x^n=\log\Big(\frac{1}{1-x}\Big),$$

valid if $|x|<1$, we see that the expression (2) equals

$$(-2k)\Big(\log\Big(\frac{1}{1+\frac{1}{k}}\Big)+\frac{1}{k}\Big)-\log\Big(\frac{1}{1+\frac{1}{k}}\Big).$$

Now we sum this from $k=1$ to $k=N$, say. After tidying up the last expression, we see that we need to calculate the sum

$$-2N+\sum_{k=1}^{N}(2k+1)\big(\log(k+1)-\log(k)\big). \tag{3}$$

This equals (we are using "partial summation" here)

$$-2N+\sum_{k=1}^{N+1}\big(2(k-1)+1\big)\log(k)-\sum_{k=1}^{N}(2k+1)\log(k)=-2N+(2N+1)\log(N+1)-2\sum_{k=1}^{N}\log(k).$$

Now $\sum_{k=1}^{N}\log(k)=\log(N!)$, which by Stirling's formula equals $\log\big(\sqrt{2\pi}e^{-N}N^{N+1/2}a_N\big)$, where $a_N\to 1$ as $N\to\infty$. So the expression (3) equals

$$\begin{aligned}-2N+(2N+1)\log(N+1)-2\Big(\log(\sqrt{2\pi})-N+\big(N+\frac{1}{2}\big)\log(N)+\log(a_N)\Big)\\ =(2N+1)\log((N+1)/N)-\log(2\pi)+\log(a_N).\end{aligned}$$

Using the above series for $\log(1/(1-x))$, for example, we see that $\log((N+1)/N)=1/N+O(1/N^2)$, and so $(2N+1)\log((N+1)/N)\to 2$ as $N\to\infty$. The result follows.

7. Let us call $\sum_{j=1}^{r}a_j$ the *weight* of the string $a_1\cdots a_r$. If $\sum_{j=1}^{r}a_j=1$, then the string consists of a single letter 1, which is of the required form.

Step 1. We first give a procedure for transforming any string $\mathbf{s}$ having repeated letters into a string of smaller weight.

If $\mathbf{s}$ has weight W, then at most $W-1$ applications of the procedure will therefore produce a string in which there are no repeated letters.

Consider a string $\mathbf{s}$ which has some repeated letters. Let m be the largest repeated letter in $\mathbf{s}$. Then we transform $\mathbf{s}$ into a string having a pair of m's with no $m+1$'s between them. For if there is a letter $m+1$ in the string, use a succession of moves of type (i) to get a string $\mathbf{s}'$ with the $m+1$ at the right hand end. Since there is no second $m+1$, there are no $m+1$'s between any two m's.

Choose two m's in $\mathbf{s}$ with no further m's between them, as near as possible and with no $m+1$'s between them. Then the string $\mathbf{s}$ contains the substring

$$a_k = m, a_{k+1}, \dots, a_{k+\ell-1}, a_{k+\ell} = m \tag{1}$$

for some $\ell \geq 1$, and $a_{k+1}, \dots, a_{k+\ell-1}$ are all not m or $m+1$.

If $\ell = 1$, then the two m's are adjacent, and we can delete one of them (a move of type (ii)), resulting in a string $\mathbf{s}'$ of weight $S - m$. Step 1 is done.

So $\ell \geq 2$, and we have as substring $m, a_{k+1}, \dots, m$. If $a_{k+1} \geq m+2$ or if $a_{k+1} \leq m-2$, then we can interchange a_{k+1} and the first m (a type (iii) move), resulting in a string $\mathbf{s}'$ having repeated m's, no repeated letters greater than m, no $m+1$ between these m's, but with the repeated m's closer together. Repeat this procedure as often as possible. That is, continue this procedure until the letter to the right of the first m is $m-1$, m, or $m+1$. By the initial choice of pair of m's, the letter to the right of the first m is $m-1$, and we have a substring of the form (1) in which $a_{k+1} = m-1$.

If $\ell = 2$, then $\mathbf{s}$ contains a substring $m, m-1, m$. But then a move of type (iv) turns this substring into $m-1, m, m-1$, and $\mathbf{s}$ into a string $\mathbf{s}'$ of weight $S-1$. Step 1 is done.

If $\ell \geq 3$ and $a_{k+\ell-1} \geq m+2$ or $a_{k+\ell-1} \leq m-2$, then we interchange $a_{k+\ell-1}$ and the right hand m. Continue this procedure until the letter to the left of the second m is $m-1$, m, or $m+1$. This letter must be $m-1$ for the same reasons that $a_{k+1} = m-1$. Now if $\ell = 3$, we have a substring $m, m-1, m-1, m$, and so a move of type (ii) removes one of the $m-1$'s, resulting in a string $\mathbf{s}'$ of weight $S-(m-1) < S$, and we have done Step 1.

If $\ell \geq 4$, we look at a_{k+2}. If $a_{k+2} \geq m+2$ or if $a_{k+2} \leq m-3$, then we can make two type (iii) moves to replace $m, m-1, a_{k+2}$ by $a_{k+2}, m, m-1$. Repeat this procedure as often as possible. That is, continue this procedure until the letter to the right of $m, m-1$ is $m-2$, $m-1$, m, or $m+1$. The cases $m-1$, m and $m+1$ are excluded as above, and so $a_{k+2} = m-2$ must hold. Similarly, if $\ell \geq 5$, $a_{k+\ell-2}$ must be $m-2$.

Continuing in this way, we obtain a substring (1) in which either $\ell = 2j+1$ is odd, and the substring is

$$m, m-1, \dots, m-j, m-j, \dots, m-1, m,$$

or $\ell = 2j$ is even, and the substring is

$$m, m-1, \dots, m-j+1, m-j, m-j+1 \dots, m-1, m.$$

In the first case, we can delete one of the $m-j$'s getting a string $\mathbf{s}'$ of weight $S-(m-j) < S$.

In the second case, we do a move of type (iv) to replace $m-j+1, m-j, m-j+1$ by $m-j, m-j+1, m-j$. This gives a string $\mathbf{s}'$ of weight $S-1 < S$.

So in all cases with a repeated letter present we can transform the string into a string of smaller weight.

Step 2. Now we show that if all the letters of the string are different, then we can reorder them so that these letters are in increasing order.

To start with, we perform some moves of type (i) to move the largest letter in the string to the right hand end. We next aim is to obtain a string of the form

$$a_1, \dots, a_{r-2}, a_{r-1}, a_r, \tag{2}$$

with $a_{r-1} < a_r$ and with all of $a_1, \ldots, a_{r-2}$ less than a_{r-1}. To do this, suppose that a_i is the largest of the letters $a_1, \ldots, a_{r-1}$. Then in particular, $a_k \leq a_i - 1$ for $k = i+1, \ldots, r-1$, and, because $a_i \leq a_r - 1$, we have $a_k \leq a_r - 2$ for $k = i+1, \ldots, r-1$. So by a succession of moves of type (iii), we can move a_r to the left until it is immediately to the right of a_i. Then by a succession of moves of type (i), we move the pair a_i, a_r to the right hand end. The string is now of the form (2).

Suppose that we have brought the string into the form

$$a_1, \ldots, a_{r-j+1}, \ldots, a_r, \tag{3}$$

with $a_{r-j+1} < \cdots < a_r$ and with all of $a_1, \ldots, a_{r-j}$ are less than a_{r-j+1}. If the largest of $a_1, \ldots, a_{r-j}$ is a_i, then as in the previous step, all the letters a_k, $i < k \leq r - j$, are at most $a_{r-j+1} - 2$. So we can move each of $a_{r-j+1}, \ldots, a_r$ to the left until they are immediately to the right of a_i. Then by a succession of moves of type (i), we move the block $a_i, a_{r-j+1}, \ldots, a_r$ to the right hand end. The string is now of the form (3), but with j increased by 1. We can continue this procedure until the letters are all in increasing order.

8. This is a result proved by J.H. Davenport in 1935. In a 1947 note, (*Journal of the London Mathematics Society*, Volume 22, 1947, pages 100-101), he remarks that the result was also proved by Cauchy in 1813.

Let $m = |A|$ and $n = |B|$. The proof is by induction on n.

If $n = 1$, then $B = \{b\}$, say, and $|A + B| = |A + b| = |A| = |A| + |B| - 1$ because the map $x \mapsto x + b$ is a bijection of $\mathbb{F}_p$.

If $n = 2$, write $B = \{b_1, b_2\}$. Suppose that $|A+B| < m+2-1$. Then $|A+B| \leq m$, and so $|A + B| = m$, because $A + B \supseteq A + b_1$, which has m elements. So $A + B = A + b_1$, and similarly $A + B = A + b_2$. Thus $A + b_1 = A + b_2$. Hence $A = A + c$, where $c = b_2 - b_1 \neq 0$. But then $A = (A+c)+c = A+2c$, and $A = (A+2c)+c = A+3c$, etc. So for $i = 0, \ldots, p-1$, $A = A + ic$. Pick any $a_0 \in A$. Then the p elements $a_0 + ic$, $0 \leq i \leq p - 1$ are distinct and all in A. So $A = \mathbb{F}_p$. So $A + b_1 = \mathbb{F}_p$ too, and since $A + B \supseteq A + b_1$, we have $A + B = \mathbb{F}_p$, so that $|A + B| = p$.

Now suppose that $n > 2$, and that the result has been proved for any subsets A and B with $|B| < n$. Now let $A, B \subset \mathbb{F}_q$, with $|A| = m$ and $|B| = n$. Form $C = A + B$, and let $\ell = |C|$. If $\ell = p$, we are done, and so suppose that $\ell < p$. Let $b, b' \in B$ be distinct, and apply the previous paragraph to C and $\{b, b'\}$. We see that $C + \{b, b'\}$ has at least $\ell + 1$ elements. Since $C + b$ and $C + b'$ both have only ℓ elements, we see that $C + b$ is not contained in $C + b'$. So there is an element $d \in C + b$ such that $d \notin C + b'$. So $d - b \in C$, but $d - b' \notin C$. Fix this d, and order the elements of B so that $B = \{b_1, \ldots, b_n\}$, with

$$d - b_i = c_i \in C \text{ for } i = 1, \ldots, r \text{ and } d - b_j \notin C \text{ for } j = r + 1, \ldots, n.$$

Here $0 < r < n$ because the above b is one of the b_i's, $i \leq r$, and the above b' is one of the b_j's, $j \geq r + 1$.

Now if $j \geq r + 1$, and if $a \in A$, then $a + b_j$ cannot equal any c_i, $i \leq r$. For otherwise

$$a + b_j = c_i = d - b_i,$$

so that

$$a + b_i = d - b_j \notin C,$$

contrary to the definition of C. So if we form $B' = \{b_{r+1}, \ldots, b_n\}$, then

$$A + B' \subset C \setminus \{c_1, \ldots, c_r\}.$$

Let $\ell' = |A + B'|$. Then the last inclusion shows that $\ell' \le \ell - r$. On the other hand, $|B'| = n - r < n$, and so by the induction hypothesis we have $\ell' \ge m + (n - r) - 1$. Hence

$$\ell - r \ge \ell' \ge m + (n - r) - 1,$$

from which we see that $\ell \ge m + n - 1$.

9. For $k \in \mathbb{N} = \{0, 1, \ldots\}$, let

$$P_k = \frac{q^k - (-q^{-1})^k}{q + q^{-1}}.$$

The first few P_k's are $P_0 = 0$, $P_1 = 1$, $P_2 = q - q^{-1} = \alpha$, $P_3 = \alpha^2 + 1$ and $P_4 = \alpha^3 + 2\alpha$. These are certainly polynomials in α with coefficients in $\mathbb{N}$. A routine calculation shows that for $k = 1, 2, \ldots$,

$$\alpha P_k + P_{k-1} = P_{k+1}.$$

So we can prove that P_k is always a polynomial in α with coefficients in $\mathbb{N}$ by induction: the assertion is true for $k = 0, 1$. Assume that $n \ge 1$ and that $P_0, \ldots, P_n$ are all polynomials in α with coefficients in $\mathbb{N}$. Then

$$P_{n+1} = \alpha P_n + P_{n-1}$$

is also a polynomial in α with coefficients in $\mathbb{N}$.

We can exhibit the polynomials explicitly. We claim that

$$P_n = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-i-1}{i} \alpha^{n-2i-1}. \tag{1}$$

We check that by induction too. If $n = 0$, then the right hand side is zero (since $\sum_{i=0}^{-1} x_i$ is by convention 0, for any x_i), as is P_0. If $n = 1$, then the right hand side of (1) is

$$\sum_{i=0}^{0} \binom{1-i-1}{i} \alpha^{1-2i-1} = 1$$

because $\binom{0}{0} = 1$. So (1) holds for $n = 1$ too. Suppose that (1) holds for $n = 0, \ldots, k$, where $k \ge 1$. Then

$$\begin{aligned}
P_{k+1} &= \alpha P_k + P_{k-1} \\
&= \alpha \sum_{i=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k-i-1}{i} \alpha^{k-2i-1} + \sum_{i=0}^{\lfloor \frac{k-2}{2} \rfloor} \binom{k-i-2}{i} \alpha^{k-2i-2} \\
&= \sum_{i=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k-i-1}{i} \alpha^{k-2i} + \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor - 1} \binom{k-i-2}{i} \alpha^{k-2i-2} \\
&= \sum_{i=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k-i-1}{i} \alpha^{k-2i} + \sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} \binom{k-i-1}{i-1} \alpha^{k-2i} \qquad (2)
\end{aligned}$$

We have used $\lfloor\frac{k-2}{2}\rfloor = \lfloor\frac{k}{2}\rfloor - 1$ here, and in the last equation replaced i by $i' = i+1$. If $1 \le i \le \lfloor(k-1)/2\rfloor$, then the coefficients of α^{k-2i} in the two sums in (2) add to give

$$\binom{k-i-1}{i} + \binom{k-i-1}{i-1} = \binom{k-i}{i}.$$

If $i = 0$, then there is a coefficient of α^{k-2i} only in the first sum in (2), and it is $\binom{k-1}{0} = 1 = \binom{k-0}{0}$.

If $\lfloor\frac{k-1}{2}\rfloor = \lfloor\frac{k}{2}\rfloor$, i.e., if k is *odd*, then we have shown that

$$P_{k+1} = \sum_{i=0}^{\lfloor\frac{k}{2}\rfloor} \binom{k-i}{i} \alpha^{k-2i}, \tag{3}$$

which is (1), with $n = k+1$. If $k = 2m$ is *even*, then for $i = m = \lfloor\frac{k}{2}\rfloor$ there is a coefficient of α^{k-2i} in (2) only in the second sum there, and it is

$$\binom{k-i-1}{i-1} = \binom{2m-m-1}{m-1} = \binom{m-1}{m-1} = 1 = \binom{k-m}{m}.$$

Hence the coefficient of α^{k-2i} in (2) is $\binom{k-i}{i}$ for all i between 0 and $m = \lfloor\frac{(k+1)-1}{2}\rfloor$, and so (3) holds in this case too. This completes the induction proof that (1) holds for all n.

10. We first show that if $x, y \in X$ satisfy $x^2 = x$ and $y^2 = y$, then $xy = yx$ must hold. To see this, let $a = y(xy)'x$. Then

$$a^2 = y(xy)'xy(xy)'x = y(xy)'x = a,$$

$$(xy)a(xy) = xyy(xy)'xxy = xy(xy)'xy = xy,$$

and

$$a(xy)a = y(xy)'xxyy(xy)'x = y(xy)'xy(xy)'x = y(xy)'x = a.$$

So $a = (xy)'$ by uniqueness. But $a = aaa$, so again by uniqueness, $a = a' = (xy)'' = xy$. Thus $(xy)^2 = a^2 = xy$. Similarly, $(yx)^2 = yx$, so $(xy)(yx)(xy) = xyxy = xy$, and similarly $(yx)(xy)(yx) = yx$. So again by uniqueness, $yx = (xy)' = xy$.

Now let $x, y \in X$, and note that $(uu')^2 = uu'$ and $(u'u)^2 = u'u$ for all $u \in X$. So using the last paragraph,

$$(xy)(y'x')(xy) = x(yy')(x'x)y = x(x'x)(yy')y = xy,$$

and

$$(y'x')(xy)(y'x') = y'(x'x)(yy')x' = y'(yy')(x'x)x' = yx,$$

so that, finally, again by uniqueness, $(xy)' = y'x'$.