Remembering Somesh

Thriyambakam Krishnan, P63, Golden Enclave, HAL (Old) Airport Road, Bangalore 560 017

Somesh Bagchi (11.09.1946 – 05.10.2012) was a mathematician of extraordinary breadth and depth. His area of research was harmonic analysis on Euclidean spaces and on Lie groups but his mastery extended to many other branches of mathematics.

Somesh Chandra Bagchi was born in Bangladesh (in what was East Pakistan) in a town called Gouripur, in the Netrokona Sub Division of Mymensingh District on 11 September 1946 to Minati and Dinesh Chandra Bagchi. He passed away in Kolkata on 5 October 2012 at the age of 66, after half a year of brave and tough battle against lung cancer and its consequent complications.

Somesh's family continued to live in East Pakistan, even after independence and the partition of Bengal into East and West Bengal, and moved to India (Kolkata, then spelt Calcutta) only after Somesh completed his matriculation in Mymensingh Zilla School. In Kolkata, Somesh completed his Pre-University at Jaipuria College, B.Sc. in Physics from St. Xavier's College, M.Stat., and Ph.D. from the Indian Statistical Institute (ISI) for his dissertation on Vector-Valued Stationary Stochastic Processes under the supervision of Prof. M. G. Nadkarni.

Somesh married Ratna (daughter of Sabita and Gopal Majumdar of Raiganj, North Dinajpur) and has a son Ramanuj. He is survived by his widow and son.

Soon after his Ph.D., he spent the years 1973–75 at the Tata Institute of Fundamental Research in Mumbai, before joining the faculty of the Indian Statistical Institute, Kolkata, where he remained until he retired as a Professor of Mathematics in 2011 at the age of 65. In all these years at the Institute, he took sabbatical leave only for a year which he spent at the University of Puget Sound in Tacomo, Washington State, USA.

Although his Bachelor's degree was in Physics and his Master's degree was in Statistics, his passion was Mathematics, which he did and taught with a great deal of commitment. Even after retiring, he taught at the Vivekananda University in Belur across the Hooghly river from Kolkata. Besides teaching regular courses at the ISI, Somesh taught regularly in various summer schools for researchers or refresher courses and nurture programs for undergraduates, all over the country, whether it was organized by the ISI or other organizations.

Somesh was a fabulous teacher at all levels. He was inspirational. His own passion for Mathematics was conveyed to his students. His lectures were lucid and extraordinarily clear. Scores of students from other institutions, including doctoral students would drop in to get his help, which he unhesitatingly gave. Despite his busy teaching schedule in the ISI and outside, he actively collaborated in research in harmonic analysis with his colleagues and guided three very good doctoral dissertations. He was a reluctant publisher of research papers, even when he had good results. He contributed to the national efforts for improvement of research and training in Mathematics as a member of the National Board for Higher Mathematics, in which capacity he participated in organizing the International Congress of Mathematicians in Hyderabad in August 2010. He was a member of the Executive Committee of the Ramanujan Mathematical Society (2010 – 2012). He never shirked administrative work and in fact carried out much more than his fair share of it, both academic and general. He was the Dean of Studies, Professor-in-Charge of the Theoretical Statistics and Mathematics Division, and he was even the Acting Director of the ISI for a brief period. Besides a great deal of teaching, he participated whole-heartedly in the admission work of setting up test papers, conducting selection tests, evaluating tests, and interviewing candidates. He was also a member of the Works Advisory Committee, Library Committee, etc. from time to time and carried out these tasks with promptness, efficiency, and good cheer and zeal.

Somesh was a great and popular story teller. He specialized in amusing his friends with witty and humorous real stories conveying the idiosycracies of our colleagues in the academic world in general and mathematicians in particular. Many a story used to get repeated on different occasions to different audiences but he had this uncanny ability to render them in precisely the same way with exactly the same words every time he repeated them! He was great company and he enlivened the great Bengali institution of adda.

Generations of grateful and admiring students, friends and colleagues spread all over the country and abroad mourn the loss of Somesh Chandra Bagchi and share the grief with his family.

Comparing Cardinalities of Sets

Arindama Singh
Department of Mathematics, Indian Institute of Technology Madras, Chennai 600 036
E-mail: asingh@iitm.ac.in

Abstract. Students often have motivational difficulty in accepting the definitions of comparing cardinalities of sets. The key to the application of the concepts lies in the so called Schröder-Bernstein theorem, the proof of which is often avoided due to its difficulty level. In this short article, we discuss the remarkable results around this theorem and finally give a very simple proof. On the way, we also construct a simple proof of uncountability of the set of real numbers, which follows directly from the completeness property.

1. Introduction

To determine the number of elements in a finite set, we count the elements. If the result is a certain natural number n, then by such a counting, we have put the set in one-one correspondence with the set $\{1, 2, 3, \ldots, n\}$. Thus even if we do not know the names of different numbers, we still can determine whether two given finite sets have the same number of elements or not. Well, we simply try to put them in one-one correspondence; if we succeed, then they have the same number of elements, else, they have different number of elements. For arbitrary sets, the *number of elements* is called *cardinality*.

In the sequel, we denote the cardinality of a set A by $|A|$. For sets A and B, we write $A - B$ instead of $A \setminus B$, which is the set of elements of A that are not in B. If $f : A \to B$ is any map, $x \in A$, and $X \subseteq A$, then we write $f(x)$ for that element in B to which f associates x, and $f(X)$ denotes the set of all elements $f(x)$ where $x \in X$. Thus $f(A)$ is the range of f. For any subset C of B, $f^{-1}(C)$ denotes the set $\{x \in A : f(x) \in C\}$. If $C \cap f(A) = \emptyset$, then $f^{-1}(C) = \emptyset$. When f is one-one and onto, $f^{-1} : B \to A$ is a map, and $f^{-1}(b) = a$ if and only if $f(a) = b$ for $a \in A$ and $b \in B$.

We agree that if A and B are sets, then $|A| = |B|$ if and only if there exists a one-one map from one onto the other. But then how to define the notion of $|A| \leq |B|$? Looking at the definition of $|A| = |B|$, it is tempting to break it into two parts, that is,

There exists a one-one map from A to B.
There exists a map from A onto B.

But there is a gap between the existence of a one-one map from A onto B and the conjunction of the two conditions above. It is quite possible that even if the above two conditions are satisfied, there may not exist a map which is both one-one and onto. It suggests to formulate another alternative of breaking $|A| = |B|$ into the following two parts:

There exists a one-one map from A to B.
There exists a one-one map from B to A.

Comparing these two formulations, we ask whether the second parts of them are equivalent or not. That is, whether the following are equivalent:

There exists a map from A onto B.
There exists a one-one map from B to A.

We see that if there exists a one-one map from B to A, then we have a bijection from B to $f(B) \subseteq A$. Then $f^{-1} : f(B) \to A$ is onto A. Now, if $A - f(B)$ is nonempty, then associate all elements in $A - f(B)$ to a particular element of B. This extension of the map f^{-1} is clearly a map from A onto B.

What about the converse? Suppose there exists a map g from B onto A. Then look at the reverse arrows of this g. For any $a \in A$, consider the set $g^{-1}(\{a\})$. Using Axiom of Choice, get an element $x_a \in g^{-1}(\{a\})$. The map that takes a to x_a is thus one-one from A to B. In the absence of the axiom of choice, it does not seem possible to prove this part.

A natural alternative is to take $|A| \leq |B|$ when there exists a one-one map from A onto a subset of B. However, this is equivalent to having a one-one map from A to B.

2. Uncountabilty

With these considerations, we compare cardinalities of sets as follows.

Definition 1. *Let A and B be sets.*
$|A| = |B|$ if there exists a one-one map from A onto B.

$|A| \le |B|$ *if there exists a one-one map from* A *to* B. $|A| \le |B|$ *is also written as* $|B| \ge |A|$.
$|A| < |B|$ *if* $|A| \le |B|$ *but* $|A| \ne |B|$. $|A| < |B|$ *is also written as* $|B| > |A|$.

If $A \subseteq B$, then the identity map $I : A \to B$ is one-one. Hence $|A| \le |B|$. The set E of all even positive numbers has cardinality less than or equal to that of $\mathbb{N}$. However, $|E| = |\mathbb{N}|$ since the map $f : \mathbb{N} \to E$ defined by $f(n) = 2n$ is a one-one and onto map. It is easy to see that for sets A, B, C, if $|A| \le |B|$ and $|B| \le |C|$, then $|A| \le |C|$ using composition of maps.

Let A be a set. A is said to be *finite* if either $A = \emptyset$ or $|A| = n = |\{1, 2, \ldots, n\}|$; A is called *denumerable* if $|A| = |\mathbb{N}|$; and A is *countable* if $|A| \le |\mathbb{N}|$. All subsets of a countable set are countable; thus all supersets of uncountable sets are uncountable. It can be shown by induction that if A is any infinite set, then $|\mathbb{N}| \le |A|$. Every finite set is countable and all infinite subsets of $\mathbb{N}$ are denumerable and thus countable. All elements of a denumerable set can be enumerated in a non-ending sequence of distinct elements:

$$x_1, x_2, \ldots, x_n, \ldots$$

The set $\mathbb{Z}$ of all integers is denumerable since the map $f : \mathbb{Z} \to \mathbb{N}$ defined by

$$f(m) = \begin{cases} -1 - 2m & \text{if } m < 0 \\ 2(1 + m) & \text{if } m \ge 0 \end{cases}$$

is a one-one and onto map. The set $\mathbb{Q}$ of all rational numbers is denumerable since it contains $\mathbb{Z}$ and the map $g : \mathbb{Q} \to \mathbb{Z}$ defined by

$$g\left(\frac{p}{q}\right) = \begin{cases} 2^p 3^q & \text{if } p \in \mathbb{N} \cup \{0\}, q \in \mathbb{N} \\ -2^p 3^q & \text{if } -p \in \mathbb{N}, q \in \mathbb{N} \end{cases}$$

is one-one; assuming that p/q is in reduced form. Wait! Have we exhibited a map from $\mathbb{Q}$ to $\mathbb{Z}$ which is one-one and onto? No! Then how do we conclude that $\mathbb{Q}$ is denumerable? By now, we have only proved that

$$|\mathbb{Q}| \le |\mathbb{Z}| \quad \text{and} \quad |\mathbb{Z}| \le |\mathbb{Q}|.$$

Does it follow that $|\mathbb{Q}| = |\mathbb{Z}|$? Yes, by Schröder-Bernstein theorem, which says the following:

> If there exist a one-map from A to B and a one-one map from B to A, then there exists a one-one map from A onto B.

We will prove this result in Section 3. What about the set $\mathbb{R}$ of real numbers? Recall that $\mathbb{R}$ is a (the) complete ordered field containing $\mathbb{Q}$. Along with the usual properties of addition, multiplication and of the order relation $\le$, it satisfies the following, called the *completeness principle*:

> Every subset of $\mathbb{R}$ which is bounded above, has a least upper bound (lub), and
> every subset of $\mathbb{R}$ which is bounded below, has a greatest lower bound (glb).

In fact, existence of lub guarantees the existence of glb and vice versa. Using this property, we give a proof of uncountability of $\mathbb{R}$.

Theorem 1. $\mathbb{R}$ *is uncountable.*

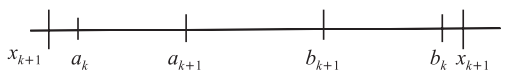
Proof. On the contrary, suppose $\mathbb{R}$ is countable. Then $[0, 1]$ is countable since $[0, 1] \subseteq \mathbb{R}$. But $[0, 1]$ is not a finite set since $f : \mathbb{N} \to [0, 1]$, defined by $f(n) = 1/n$, is one-one. Hence $[0, 1]$ is denumerable. Then, let

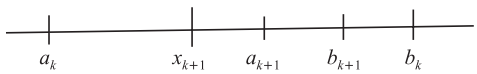
$$x_1, x_2, \ldots, x_n, \ldots$$

be an enumeration of $[0, 1]$. For each $n \in \mathbb{N}$, construct a sub-interval $[a_n, b_n]$ of $[0, 1]$ that does not contain x_n, inductively, as in the following:

> Initially, set $a_0 := 0, b_0 := 1$.
> Suppose, for $k \ge 0$, a_k, b_k have already been chosen.
> Choose a_{k+1}, b_{k+1} as follows:
> If $a_k < x_{k+1} < b_k$, then $y_k := x_{k+1}$, else, $y_k := a_k$.
> $a_{k+1} := y_k + (b_k - y_k)/3,\ b_{k+1} := y_k + 2(b_k - y_k)/3$.

The construction says that if x_{k+1} lies in the open interval (a_k, b_k), then choose the interval $[a_{k+1}, b_{k+1}]$ as the middle third of $[x_{k+1}, b_k]$; and if $x_{k+1} \le a_k$ or $x_{k+1} \ge b_k$, then choose $[a_{k+1}, b_{k+1}]$ as the middle third of $[a_k, b_k]$.





We observe that for each $n \in \mathbb{N}$, $[a_n, b_n] \ne \emptyset$ and $x_n \notin [a_n, b_n]$. Moreover,

$$0 < a_1 < a_2 \cdots < a_n < \cdots < \cdots < b_n < \cdots < b_2 < b_1 < 1.$$

Write $a = \text{lub}\,\{a_n : n \in \mathbb{N}\}$ and $b = \text{glb}\,\{b_n : n \in \mathbb{N}\}$. Then, $0 < a \leq b < 1$. Thus $[a, b]$ is a nonempty sub-interval of $[0, 1]$. Moreover,

$$x_n \notin [a_n, b_n] \supseteq [a, b] \quad \text{for each } n \in \mathbb{N}.$$

That is, no number in $[a, b]$ is enumerated in the assumed enumeration, a contradiction. □

It can be shown that each real number has a decimal expansion; see [1]. This representation is not unique since any number having a finite number of digits after the decimal point does have exactly another representation having an infinite number of digits after the decimal point. For example, $0.12 = 0.11999\cdots$. We agree to always use the infinite one whenever a choice exists. The usual proof of uncountability of the semi-open interval $(0, 1]$ uses the *diagonalization method* of Cantor, which we now explain. Suppose, on the contrary, that $(0, 1]$ is countable. Then we have an enumeration of all numbers in $(0, 1]$ as

$$\begin{gathered} 0.a_{11}\,a_{12}\,a_{13}\,\cdots\,a_{1n}\,\cdots \\ 0.a_{21}\,a_{22}\,a_{23}\,\cdots\,a_{2n}\,\cdots \\ \vdots \\ 0.a_{n1}\,a_{n2}\,a_{n3}\,\cdots\,a_{nn}\,\cdots \\ \vdots \end{gathered}$$

where each a_{ij} is a digit ranging from 0 to 9, and in which a finite decimal ends with 9s rather than 0s. It is of course immaterial whether we choose ending with 0s or 9s, but we must resort to one and not the other so that repetitions are avoided. We then construct a decimal number

$$0.b_1b_2b_3\cdots b_n\cdots$$

where $b_i = 0$ if $a_{ii} = 9$ else $b_i = a_{ii} + 1$. Then this new decimal number is in $(0, 1]$ but it differs from each in the list above. Therefore, no enumeration of numbers in $(0, 1]$ can have all the numbers in $(0, 1]$.

Another proof uses the representation of any real number as a binary decimal. Once again, we choose to use a binary decimal number with an infinite number of digits and discard one with finite number of digits after the decimal point, if such a choice exists. The uncountability of the closed interval $[0, 1]$ is accomplished by showing that $\mathcal{P}(\mathbb{N})$, the power set of $\mathbb{N}$ and $[0, 1]$ are in one-one correspondence; and then resorting to Cantor's theorem that for any set A, $|\mathcal{P}(A)| > |A|$.

To see that $|\mathcal{P}(\mathbb{N})| \leq |[0, 1]|$, define $f : \mathcal{P}(\mathbb{N}) \to [0, 1]$ as follows.

> Let $S \subseteq \mathbb{N}$. Let $n \in \mathbb{N}$. Then $f(S)$ is the decimal number $0.a_1a_2\cdots$ in base 10 such that its nth digit $a_n = 3$ if $n \in S$, and $a_n = 4$ if $n \notin S$.

For example, $f(\{1, 2, 3\}) = 0.3334444\cdots$. Notice that f is not an onto map since for no subset A of $\mathbb{N}$, $f(A) = 0.1$. Clearly f is one-one. Hence $|\mathcal{P}(\mathbb{N})| \leq |[0, 1]|$.

For the other inequality, define $g : [0, 1] \to \mathcal{P}(\mathbb{N})$ by

> Let $x = 0.b_1b_2\cdots \in [0, 1]$, where $b_i \in \{0, 1\}$. Then $g(x) = \{i \in \mathbb{N} : b_i = 1\}$.

For example, $g(0.10111\cdots) = \{1, 3, 4, 5, \dots\}$. Again, notice that g is not an onto map, since there is no binary decimal $a \in [0, 1]$ such that $g(a) = \{1, 2\}$. For, according to the definition of g, the only suitable number a would have been 0.11, which has been discarded in favour of $0.10111\cdots$. Obviously, g is one-one. Hence $|[0, 1]| \leq |\mathcal{P}(\mathbb{N})|$.

By Schröder-Bernstein theorem, $|\mathcal{P}(\mathbb{N})| = |[0, 1]|$. It remains to prove Cantor's theorem.

Theorem 2 (Cantor). *For any set A, $|A| < |\mathcal{P}(A)|$.*

Proof. Let A be any set. The function $f : A \to \mathcal{P}(A)$ defined by $f(x) = \{x\}$ is a one-one map. Therefore, $|A| \leq |\mathcal{P}(A)|$. We next show that no function from A to $P(A)$ can be onto. On the contrary, suppose that $g : A \to \mathcal{P}(A)$ is an onto map. Notice that for any $x \in A$, $g(x) \subseteq A$. Let $B = \{x \in A : x \notin g(x)\}$. Since g is an onto map, there exists $y \in A$ such that $B = g(y)$. Then $y \in B$ iff $y \notin g(y)$ iff $y \notin B$, a contradiction. □

$\mathbb{R}$ and $\mathbb{N}$ are not in one-one correspondence. But $\mathbb{R}$ and the open interval $(0, 1)$ are in one-one correspondence, since the map $f : (0, 1) \to \mathbb{R}$ defined by

$$f(x) = \tan(-(\pi/2) + \pi\, x)$$

is one-one and onto. If you accept Schröder-Bernstein theorem, then it is trivial to guarantee the existence of a one-one map from $[0, 1]$ onto $\mathbb{R}$. Can you construct a one-one map from $[0, 1]$ onto $\mathbb{R}$?

Notice that Cantor's theorem establishes a hierarchy of infinities:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| <, \dots$$

It raises the question whether there exists a set whose cardinality is in between those of $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$? Cantor conjectured that there exists no such set, however he could not prove it. Later it was shown by Gödel that the truth of this conjecture is consistent with ZFC, a widely accepted formalization of set theory by Zermelo and Fraenkel. Cohen proved that the falsity of this conjecture is also consistent with ZFC. These two proofs established the independence of this conjecture from ZFC. Thus, the conjecture is considered a hypothesis, the *continuum hypothesis*. The generalized continuum hypothesis states that if A is any infinite set, then there does not exist a set B such that $|A| < |B| < |\mathcal{P}(A)|$. It is not yet known whether there exists a formalization of set theory in which (generalized) continuum hypothesis becomes a theorem; see [5].

Another consequence of Cantor's theorem is that the collection of all sets is not a set. For, suppose that S is the set of all sets. Then $\mathcal{P}(S) \subseteq S$. In that case, $|\mathcal{P}(S)| \leq |S|$, contradicting Cantor's theorem. This also shows that we cannot build a set corresponding to every property. For otherwise, the property "x is a set" would define the set of all sets. In fact, as the history goes, this concerns gave rise to various formalizations of set theory, one of which is ZFC.

Central to this discussion is comparing cardinalities, which rests on Schröder-Bernstein Theorem.

3. Cantor-Schröder-Bernstein Theorem

As to the name of this section, Cantor first formulated the theorem and gave a proof relying on the well ordering principle; this principle, as we know, is equivalent to the axiom of choice. Schröder gave a proof without using the axiom of choice, in which there were gaps. The first published correct proof without using the axiom of choice was by Bernstein, though it is said that Dedekind proved it a bit earlier but did not publish. Zermelo and König have also proved the theorem; see [2,4]. All these proofs reveal partitions of the sets into a fixed finite number of parts each, where the individual parts of both the sets are in one-one correspondence. This is the content of Banch-Mapping theorem, where the sets are partitioned into two subsets. We prove this first.

Theorem 3 (Banach Mapping). *Let A, B be nonempty sets. Let $f : A \to B$ and $g : B \to A$ be functions. Then there exist subsets A_1, A_2 of A and subsets B_1, B_2 of B such that*

$$A_2 = A - A_1,\ B_2 = B - B_1,\ f(A_1) = B_1,\ g(B_2) = A_2.$$

Proof. Consider the collection

$$\mathcal{C} = \{D \subseteq A : g(B - f(D)) \subseteq A - D\}.$$

$f(\emptyset) = \emptyset$. $B - f(\emptyset) = B$. $g(B - f(\emptyset)) = g(B) \subseteq A = A - \emptyset$. Hence, $\emptyset \in \mathcal{C}$. That is, $\mathcal{C}$ is a nonempty collection. Define

$$E = \cup_{D \in \mathcal{C}} D.$$

Now,

$$\begin{aligned} g(B - f(E)) &= g(B - f(\cup_{D\in\mathcal{C}} D)) = g(B - \cup_{D\in\mathcal{C}} f(D)) \\ &= g(\cap_{D\in\mathcal{C}}(B - f(D))) \\ &\subseteq \cap_{D\in\mathcal{C}}(g(B - f(D))) \subseteq \cap_{D\in\mathcal{C}}(A - D) \\ &= A - \cup_{D\in\mathcal{C}} D = A - E. \end{aligned}$$

That is,

$$g(B - f(E)) \subseteq A - E.$$

We want to show that $g(B - f(E)) = A - E$. On the contrary, suppose $g(B - f(E)) \neq A - E$. Then there exists an $x \in A - E$ such that $x \notin g(B - f(E))$. The conditions $x \notin g(B - f(E))$ and $g(B - f(E)) \subseteq A - E$ imply that

$$g(B - f(E)) \subseteq A - (E \cup \{x\}).$$

Since $f(E) \subseteq f(E \cup \{x\})$, $B - f(E \cup \{x\}) \subseteq B - f(E)$. Then

$$g(B - f(E \cup \{x\})) \subseteq g(B - f(E)) \subseteq A - (E \cup \{x\}).$$

That is, $E \cup \{x\} \in \mathcal{C}$. As $E = \cup_{D\in\mathcal{C}} D$, $E \supseteq E \cup \{x\}$. That is, $x \in E$, This contradicts $x \in A - E$.

We conclude that $g(B - f(E)) = A - E$.

Finally, take $E = A_1$, $A - E = A_2$, $B_1 = f(E)$ and $B_2 = B - f(E)$. □

Cantor-Schröder-Bernstein theorem can be derived from Theorem 2 by defining the map $h : A \to B$ with $h(x) = f(x)$ for $x \in A_1$ and $h(x) = g^{-1}(x)$ for $x \in A_2$. Notice that $f : A_1 \to B_1$ is one-one and onto; so is the map $g : B_2 \to A_2$. Therefore, $h : A \to B$ is one-one and onto.

The proof of Banach mapping theorem constructs the set $E \subseteq A$ satisfying

$$g(B - f(E)) = A - E.$$

That is, $E = A - g(B - f(E))$. It means that if $\phi(X) = A - g(B - f(X))$ for subsets X of A, then E is a fixed point of this map ϕ. But under what condition(s) a map ϕ taking subsets of A to subsets of A will have a fixed point? The proof of Theorem 2 suggests this condition.

Theorem 4 (Knaster Fixed Point). *Let $\mathcal{P}(A)$ denote the power set of a nonempty set A. Let a map $\psi : \mathcal{P}(A) \to \mathcal{P}(A)$ satisfy*

$$X \subseteq Y \text{ implies } \psi(X) \subseteq \psi(Y) \quad \text{for} \quad X, Y \subseteq A.$$

Then there exists $G \subseteq A$ such that $\psi(G) = G$.

Proof. The collection $\mathcal{K} = \{X \subseteq A : X \subseteq \psi(X)\}$ of subsets of A is nonempty since $\emptyset \subseteq \psi(\emptyset)$. Define

$$G = \cup_{Y \in \mathcal{K}} Y.$$

It says that each set in $\mathcal{K}$ is a subset of G. Now,

$$G = \cup_{Y \in \mathcal{K}} Y \subseteq \cup_{Y \in \mathcal{K}} \psi(Y) = \psi(\cup_{Y \in \mathcal{K}} Y) = \psi(G).$$

If $G \neq \psi(G)$, then there exists $x \in \psi(G)$ such that $x \notin G$. Since $G \subseteq \psi(G)$ and $x \in \psi(G)$, we see that

$$G \cup \{x\} \subseteq \psi(G) \subseteq \psi(G \cup \{x\}).$$

That is, $G \cup \{x\} \in \mathcal{K}$. Hence $G \cup \{x\} \subseteq G$. That is, $x \in G$, a contradiction.

Therefore, $\psi(G) = G$. □

Generalization has made the things simpler. The proof of Theorem 3 looks simpler than that of Theorem 2. To derive Theorem 2 from Theorem 3, all that we do is take a particular map ψ which satisfies the required condition. For this purpose, define the map $\psi : P(A) \to P(A)$ by

$$\psi(X) = A - g(B - f(X)) \quad \text{for} \quad X \subseteq A.$$

Now,

$$\begin{aligned} X \subseteq Y &\Rightarrow f(X) \subseteq f(Y) \Rightarrow B - f(X) \supseteq B - f(Y) \\ &\Rightarrow g(B - f(X)) \supseteq g(B - f(Y)) \\ &\Rightarrow A - g(B - f(X)) \subseteq A - g(B - f(Y)). \end{aligned}$$

That is, $X \subseteq Y$ implies $\psi(X) \subseteq \psi(Y)$. An application of Theorem 3 completes the proof of Theorem 2.

In fact, Knaster fixed point theorem holds true in a much more general setting. Suppose A is a partially ordered set with a partial order $\leq$. It is called a *complete lattice* if every subset of A has an infimum and a supremum with respect to the partial order. We say that a map $\phi : A \to A$ is *order preserving* if $\phi(x) \leq \phi(y)$ whenever $x \leq y$. Then Knaster-Tarski fixed point theorem can be stated as follows:

> Every order preserving map on a complete lattice has a fixed point.
> Further, the set of all such fixed points of the map is a complete lattice.

The proof of this result is similar to that of Theorem 3, but is to be formulated in terms of the generalized notions appropriate to a complete lattice. Moreover, the converse of Knaster-Tarski fixed point theorem for lattices holds. It states that a lattice, i.e., a partially ordered set in which every finite subset has a minimum and a maximum, is complete if each order preserving map has a fixed point.

The generalizations have helped in constructing an independent proof of Cantor-Schröder-Bernstein theorem, which we give below. Find out in the proof, how the ideas of fixed point and partition of the sets are in action.

Theorem 5 (Cantor-Schröder-Bernstein). *Let A and B be nonempty sets. Let $f : A \to B$ and $g : B \to A$ be one-one functions. Then there exists a function $h : A \to B$, which is both one-one and onto.*

Proof. Define $S = (A - g(B)) \cup \cup_{n \in \mathbb{N}} (g \circ f)^n (A - g(B))$. See the figure below. Then $S = (A - g(B)) \cup (g \circ f)(S) \subseteq A$. Since $g(B) \subseteq A$ and $(g \circ f)(S) \subseteq A$, we obtain

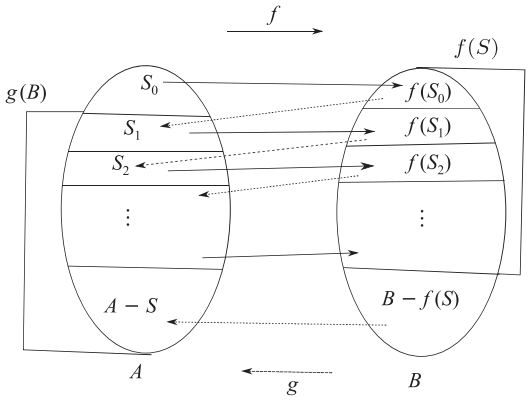
$$\begin{aligned} A - S &= A - ((A - g(B)) \cup (g \circ f)(S)) \\ &= (A - (A - g(B)) - (g \circ f)(S) \\ &= g(B) - g(f(S)) = g(B - f(S)). \end{aligned}$$

The last equality follows since g is one-one. Hence $g : B - f(S) \to A - S$ is one-one and onto. Also, $f : S \to f(S)$ is one-one and onto. Hence the map $h : A \to B$ defined by

$$h(x) = \begin{cases} f(x) & \text{for } x \in S \\ g^{-1}(x) & \text{for } x \in A - S \end{cases}$$

is both one-one and onto. □

Compare this proof with the classical one in text books on Set Theory, for example, in [1]. For completeness, prove the facts contained in the following exercise.



$S_0 = A - g(B), S_1 = g(f(S_0)), S_2 = g(f(S_1)), \ldots, S = \cup S_i$

Exercise. Let $f : A \to B$ be a function where A and B are nonempty sets. Suppose that $A_1 \subseteq A$ and $A_2 \subseteq A$.

1. If $A_1 \subseteq A_2$, then $f(A_1) \subseteq f(A_2)$.
2. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
3. $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. Equality holds if f is one-one.
4. $f(A_1 - A_2) \supseteq f(A_1) - f(A_2)$. Equality holds if f is one-one.
5. Formulate and prove (2)–(3) when the operations of union and intersection are taken over a collection of subsets of A.

Acknowledgment

I thank Prof. S. Kumaresan of the University of Hyderabad, who wished that I write this article for the benefit of students, and Prof. G. P. Youvaraj who wished to see this proof of uncountability of $\mathbb{R}$ in print. I also thank the referee for his/her suggestions, which improved the presentation of the paper.

References

[1] D. S. Bridges, Foundations of real and abstract analysis, Springer Verlag, New York (1997).

[2] M. Eigner and G. M. Ziegler, Proofs from the book, Springer Verlag, Fourth Ed., Berlin Heidelberg (2010).

[3] P. R. Halmos, Naive set theory, Springer Verlag, New York, 1974, First Indian Reprint (2009).

[4] A. Hinkis, Proofs of the Cantor-Bernstein Theorem: A Mathematical Excursion, Birkhauser, New York (2013).

[5] I. Stewart and D. Tall, The Foundations of Mathematics, Oxford University Press, London (2000).

Ramanujan's Awesome Sums

B. Sury

Stat-Math Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560 059

E-mail: sury@isibang.ac.in

Abstract. In 1918, Ramanujan published a paper where he proved several nice properties of certain finite sums which are now known as Ramanujan sums. Ramanujan sums have numerous other applications in combinatorics and graph theory. Further, in physics, they have applications in the processing of low-frequency noise and in the study of quantum phase locking. In this exposition, we describe some beautiful properties of these sums and discuss some of their applications.

Keywords. Ramanujan sum, cyclotomic polynomial, Ramanujan expansion, Cayley graph, roots of unity

2001 Mathematics Subject Classification: 11A25; 05A15

Introduction

In his famous paper ([SR]), Ramanujan discussed the properties of certain finite sums – the so-called Ramanujan sums. Even though Dirichlet and Dedekind had already considered these sums in the 1860's, according to G. H. Hardy, Ramanujan was the first to appreciate the importance of the sum and to use it systematically. Ramanujan sums play a key role in the proof of a famous result due to Vinogradov asserting that every large odd number is the sum of three primes.

These sums have numerous other applications in diverse branches of mathematics as well as in some parts of physics. So, what are these sums?

For integers $n \geq 1, k \geq 0$, the sum

$$c_n(k) = \sum_{(r,n)=1; r \leq n} e^{2ikr\pi/n}$$

is called a Ramanujan sum. In other words, it is simply the sum of the k-th powers of the primitive n-th roots of unity – 'primitive' here means that the number is not an m-th root of unity for any $m < n$. Note that the primitive n-th roots of unity are the numbers $e^{2ikr\pi/n}$ for all those $r \leq n$ which are relatively prime to n. The first remarkable property they have is that they are integers. Ramanujan showed that several arithmetic functions (that is, functions defined from the set of positive integers to the set of complex numbers) have 'Fourier-like' of expansions in terms of the sums; hence, nowadays these expansions are known as Ramanujan expansions. They often yield very pretty elementary number-theoretic identities. Recently, the theory of group representations of the permutation groups (specifically, the so-called super-character theory as in [FGK]) has been used to re-prove old identities in a quick way and also, to discover new identities. Thus, this subject is very much alive.

1. Properties of Ramanujan Sums

It is convenient to write

$$\Delta_n = \{e^{2ir\pi/n} : (r, n) = 1, 1 \leq r \leq n\}$$

Then, the set of all n-th roots of unity $\{e^{2ik\pi/n} : 0 \leq k < n\}$ is a union of the disjoint sets Δ_d as d varies over the divisors of n. This is because an n-th root of unity is a primitive d-th root of unity for a unique divisor d of n. It is also convenient to introduce the 'characteristic' function $\delta_{k|n}$ which has the value 1 when k divides n and the value 0 otherwise. Before stating some properties of the $c_k(n)$'s, let us recall two arithmetic functions which are ubiquitous in situations where elementary number-theoretic counting is involved. The first one is Euler's totient function

$$\phi(n) = |\{r : 1 \leq r \leq n, (r, n) = 1\}|.$$

The other arithmetic function is the Möbius function defined by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ (-1)^k, & \text{if } n = \prod_{i=1}^{k} p_i \\ 0, & \text{otherwise.} \end{cases}$$

The Möbius function keeps tab when we use the principle of inclusion-exclusion to do counting. The basic result which can be easily proved by induction on the number of prime factors, is the Möbius inversion formula:

If g is an arithmetic function and

$$f(n) = \sum_{d|n} g(d),$$

then

$$g(n) = \sum_{d|n} f(d)\mu(n/d).$$

With these notations, here are some elementary properties of the Ramanujan sums.

Properties of $c_k(n)$

(i) $c_n(k) = c_n(-k) = c_n(n-k)$.

(ii) $c_n(0) = \phi(n)$ and $c_n(1) = \mu(n)$.

(iii) $c_n(ks) = c_n(k)$ if $(s, n) = 1$. In particular, $c_n(s) = \mu(n)$ if $(s, n) = 1$.

(iv) $c_n(k) = c_n(k')$ if $(k, n) = (k', n)$. In particular, $c_n(k) \equiv c_n(k') \bmod n$ if $k \equiv k' \bmod n$.

(v) $\sum_{k=0}^{n-1} c_n(k) = 0$.

(vi) $\sum_{d|n} c_d(k) = \delta_{n|k} n$ and $c_n(k) = \sum_{d|n} d\mu(n/d)\delta_{d|k} = \sum_{d|(n,k)} d\mu(n/d)$; in particular, for prime powers p^r, we have

$$c_{p^r}(k) = \begin{cases} p^r - p^{r-1}, & \text{if } p^r | k; \\ -p^{r-1}, & \text{if } p^{r-1} || k; \\ 0, & \text{otherwise.} \end{cases}$$

(vii) $c_{mn}(k) = c_m(k)c_n(k)$ if $(m, n) = 1$.

(viii) $\sum_{k=1}^{n} c_m(k)c_n(k) = \delta_{mn} n\phi(n)$.

The property (vi) shows that these sums actually have integer values.

The proof of (i) follows already from the definition and, so do the first parts of (ii) and (iii). The second parts of (ii), (iii) as well as the assertions (iv) and (vii) will follow from (vi). We shall prove (v) and (vi).

For (v), we have

$$\sum_{k=0}^{n-1} c_n(k) = \sum_{k=0}^{n-1} \sum_{\zeta \in \Delta_n} \zeta^k = \sum_{\zeta \in \Delta_n} \sum_{k=0}^{n-1} \zeta^k = 0$$

where the last equality is because

$$\sum_{k=0}^{n-1} \zeta^k = \frac{1-\zeta^n}{1-\zeta} = 0$$

for each $\zeta \in \Delta_n$.

For proving (vi), we note that the second statement follows from the first by the Möbius inversion formula. Let us prove the first one now. We have

$$\sum_{d|n} c_d(k) = \sum_{d|n} \sum_{\zeta \in \Delta_d} \zeta^k = \sum_{m=0}^{n-1} e^{2imk\pi/n}$$

because, as we observed, the disjoint union of Δ_d as d varies over the divisors of n is the set of all n-th roots of unity. Now, if the above sum $\sum_{m=0}^{n-1} e^{2imk\pi/n}$ is multiplied by $e^{2ik\pi/n}$, we get the same sum which means that it is equal to 0 unless $n|k$. When $k|n$, the sum is clearly equal to n. This proves (vi).

The other parts easily follow from (vi).

Von Sterneck's Function

The equality $c_n(k) = \sum_{d|n} d\mu(n/d)\delta_{d|k}$ is very useful.[1] For instance, if n is a prime power p^r, as we noted above in (vi), we have

$$c_{p^r}(k) = p^r \delta_{p^r|k} - p^{r-1}\delta_{p^{r-1}|k}.$$

Using this expression in (vii) above, we get

$$c_n(k) = \frac{\mu\left(\frac{k}{(k,n)}\right)\phi(n)}{\phi\left(\frac{k}{(k,n)}\right)}.$$

The right hand side was studied by R. D. Von Sterneck in 1902 and is known by his name. The equality above itself was known before Ramanujan and is due to J. C. Kluyver in 1906.

2. Connection with Cyclotomic Polynomials

The cyclotomic polynomials $\Phi_n(x) = \prod_{\zeta \in \Delta_n}(x-\zeta)$ have some fascinating properties and have surprising consequences (see [BS], where applications such as the infinitude of primes in arithmetic progressions of the form $\{1+an\}$ are proved). We have:

$$x^n - 1 = \prod_{d|n} \prod_{\zeta \in \Delta_d} (x-\zeta) = \prod_{d|n} \Phi_d(x)$$

and – by Möbius inversion, we deduce

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Taking the logarithmic derivative, we obtain

$$\frac{\Phi_n'(x)}{\Phi_n(x)} = \sum_{d|n} \frac{dx^{d-1}\mu(n/d)}{x^d - 1}.$$

Multiplying by $x(x^n-1)$, we get a polynomial in x, viz.,

$$x(x^n-1)\frac{\Phi_n'(x)}{\Phi_n(x)} = \sum_{d|n} d\mu(n/d)(x^d + x^{2d} + \cdots + x^n).$$

Thus, the coefficient of x^k in the polynomial on the right is $\sum_{d|(n,k)} d\mu(n/d)$, which is simply the Ramanujan sum $c_n(k)$. Hence, we have:

Proposition. *For each $k < n$, the Ramanujan sum $c_n(k)$ is the coefficient of x^{k-1} in the polynomial $(x^n-1)\frac{\Phi_n'(x)}{\Phi_n(x)}$.*

3. Ramanujan Expansions of Arithmetic Functions

An arithmetic function $f(n)$ is often stored in terms of the generating function $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ which is a function of a variable s. Instead of a power series, one uses these type of series – called Dirichlet series – in this set-up. One reason is that the product of two such series produces the "*convolution*" of the corresponding arithmetic functions $f(n), g(n)$ which is something that appears naturally in number theory. That is, if f, g are two arithmetic functions and $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ and $G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$, then

$$G(s)F(s) = \sum_{n=1}^{\infty} \frac{\sum_{d|n} f(d)g(n/d)}{n^s}.$$

One writes this new multiplication (the 'convolution') as

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

Under this multiplication, the set of all arithmetic functions forms what is called a "commutative algebra with unit". In other words, with the obviously defined addition of

[1] Note that even computationally the defining sum for $c_n(k)$ requires approximately n operations whereas the other sum requires roughly $\log(n)$ operations.

arithmetic functions, the set of arithmetic functions form a complex vector space and this multiplication is compatible with that vector space structure. The unit element is the arithmetic function $\delta(n) = \delta_{n|1}$ in the notation we have used above.

Ramanujan found 'natural' expansions of standard arithmetic functions in terms of the $c_n(k)$'s as infinite series. "Natural" here is not a precisely defined notion. For instance, for an arithmetic function f, one may look for a series $\sum_{n=1}^{\infty} \widehat{f(n)} c_n(r)$ converging point-wise to f. This kind of convergence has been established so far only for a restricted class of arithmetic functions. Later researchers have tried to produce "exotic" Ramanujan expansions for several arithmetic functions which include those obtained classically by Ramanujan. It should be borne in mind that in general such an expansion may not be unique because one has equalities like $\sum_{n=1}^{\infty} \frac{c_n(k)}{n} = 0$.

We stick to giving some examples and later discuss certain classes of functions which have unique Ramanujan expansions.

Examples.

- Let $\sigma_r(k) := \sum_{d|k} d^r$ for all $r \geq 1$. Then

$$\frac{\sigma_r(k)}{k^r} = \sum_{d|k} \frac{1}{d^r} = \sum_{d=1}^{\infty} \frac{1}{d^{r+1}} \sum_{n|d} c_n(d)$$

$$= \sum_{n=1}^{\infty} \frac{c_n(k)}{n^{r+1}} \sum_{m=1}^{\infty} \frac{1}{m^{r+1}} = \zeta(r+1) \sum_{n=1}^{\infty} \frac{c_n(k)}{n^{r+1}}$$

  where $\zeta(s)$ denotes the sum of the series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ for any real $s > 1$.

- The divisor function $d(k) = \sum_{d|k} 1$ has an expansion

$$d(k) = \sum_{n=1}^{\infty} -c_n(k) \frac{\log(n)}{n}$$

- For any $m \geq 1$, a generalization of the Euler totient function is Jordan's function

$$\phi_m(k) = k^m \prod_{p|k} (1 - p^{-m}),$$

  where the product on the right is over all the prime divisors of k. Note that ϕ_1 is the Euler totient function. Ramanujan showed for any $m \geq 1$ that

$$\phi_m(k) = \frac{k^m}{\zeta(m+1)} \sum_{n=1}^{\infty} \frac{\mu(n) c_n(k)}{\phi_{m+1}(n)}.$$

- Let $r_m(k) = |\{(a, b) : a, b \in \mathbf{Z}, a^m + b^m = k\}|$, the number of ways to write k as a sum of two m-th powers. Then, Ramanujan obtained expressions for r_2, r_4, r_6, r_8 and a few other related arithmetic functions. For $r_2(k)$, this is:

$$r_2(k) = \pi \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{2n-1} c_{2n-1}(k)$$

Note the curiosity that a form of the famous prime number theorem is the assertion that $\sum_n \frac{\mu(n)}{n} = 0$ and this is also equivalent to the assertion that $\sum_{n \geq 1} \frac{c_n(k)}{n} = 0$ for all k!

Unique Ramanujan Expansions for 'even' Functions

Recall that $c_n((k, n)) = c_n(k)$; thus, for each fixed n, one may say that the function $k \mapsto c_n(k)$ is "*even modulo n*". This is in analogy with even functions which are 'even modulo 2'. The beautiful general theorem which holds good is the following one.

Theorem. *Let n be a fixed positive integer and let f be any arithmetic function which is even modulo n. Then, there exist unique numbers a_d for each $d|n$ which satisfy*

$$f(k) = \sum_{d|n} a_d c_d(k).$$

In fact, for each $d|n$, we have

$$a_d = \frac{1}{n} \sum_{e|n} f(n/e) c_e(n/d).$$

This pretty theorem has a tedious though elementary proof but the theory of super-characters mentioned in the introduction gives a very quick proof. We do not discuss the proof here but state some identities which follow quickly in that set-up.

Orthogonality Relations

- $\sum_{r|n} \phi(r) c_d(n/r) c_e(n/r) = n\phi(d)$ or 0 according as to whether $d = e$ or not.
- $\sum_{r|n} \frac{1}{\phi(r)} c_r(n/d) c_r(n/e) = \frac{n}{\phi(d)}$ or 0 according as to whether $d = e$ or not.
- If $(mu, nv) = 1$, then $c_{mn}(uv) = c_m(u) c_n(v)$.
- $\sum_{d|n} c_d(n/d) = \sqrt{n}$ or 0 according as to whether n is a perfect square or not.
- $c_d(n/e)\phi(e) = c_e(n/d)\phi(d)$ if d, e are divisors of n.
- $\sum_{d,e|n} c_d(n/e) c_e(n/d) = nd(n)$ for divisors d, e of n.

Mixed Orthogonality Relations

- For divisors d, e of n, we have $\sum_{r|n} c_d(n/r)c_r(n/e) = n$ or 0 according as to whether $d = e$ or not.
- For a divisor d of n, we have $\sum_{r|n} c_d(n/r)\mu(r) = n$ or 0 according as to whether $d = n$ or not.

A Matrix of Ramanujan Sums

Theorem. *For any $n > 1$, consider the $d(n)$ divisors of n and fix them in some order. Look at the $d(n) \times d(n)$ matrix C whose (d, e)-th entry is $c_d(e)$ for divisors d, e. Then, we have:*

The determinant of the above matrix C is $n^{d(n)/2}$ and the inverse matrix has (d, e)-th entry $\frac{1}{n}c_{n/d}(n/e)$.

Proof. Consider the 'divisibility' matrix X of size $d(n) \times d(n)$ whose (d, e)-th entry is 1 if $d|e$ and 0 otherwise. Note that X^{-1} has (d, e)-th entry is $\mu(e/d)$ if $d|e$ and 0 otherwise. This simply follows from the equality

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1. \end{cases}$$

If D is the diagonal matrix whose (d, d)-th entry is d for each $d|n$, then we have

$$XD(X^t)^{-1} = C$$

because (d, e)-th entry of the left hand side is $\sum_{r|(d,e)} r\mu(e/r)$ which we know to be equal to $c_d(e)$. This also shows that the determinant is as asserted. We may compute $C^{-1} = X^t DX^{-1}$ and get the result as asserted. □

Note that the equality $CC^{-1} = I$ expresses the identity $\sum_{r|n} c_{n/r}(d)c_{n/d}(r) = n$ or 0 according as to whether $d = n$ or not.

Finally, we end this section with the following beautiful statement which is a consequence of the theory of super-characters:

Theorem. *If $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, and the divisors of n are arranged in any fixed order, then consider, as above, the $d(n) \times d(n)$ matrix A with (d, e)-th entry $c_d(n/e)$. Then, $\det A = n^{d(n)/2}(-1)^{\sum_{i=1}^{r}[(\alpha_i+1)/2]d(n)/(\alpha_i+1)}$.*

4. A Graph-Theoretic Interpretation

Both in graph theory and in group theory, the Cayley graphs figure prominently ([KS]). If G is a group generated by a subset S which is symmetric – that is, $S = \{s^{-1} : s \in S\}$ – then, one forms the Cayley graph $\mathrm{Cay}(G, S)$ whose vertices are elements of G and, elements g, h are connected by an (undirected) edge $\overline{gh}$ if and only if $gh^{-1} \in S$.

Consider the Cayley graph $\mathrm{Cay}(\mathbf{Z}_n, \mathbf{Z}_n^*)$ where $\mathbf{Z}_n^*$ is the group of all units in $\mathbf{Z}_n$. In other words, this is a graph whose vertices can be identified with $\{0, 1, \dots, n-1\}$ and one connects i and j if and only if $i - j$ is relatively prime to n. The adjacency matrix of this graph has a very nice form – it is a circulant matrix. This matrix is

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

where $a_i = 1$ or 0 according as whether i is relatively prime to n or not. Evidently, the vectors $v_k = (1, e^{2ik\pi/n}, e^{4ik\pi/n}, \dots, e^{2(n-1)ik\pi/n})$ are linearly independent for $k = 0, 1, \dots, n-1$ and satisfy

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix} \begin{pmatrix} 1 \\ e^{2ik\pi/n} \\ \vdots \\ e^{2(n-1)ik\pi/n} \end{pmatrix}$$

$$= \lambda_k \begin{pmatrix} 1 \\ e^{2ik\pi/n} \\ \vdots \\ e^{2(n-1)ik\pi/n} \end{pmatrix}$$

where $\lambda_k = \sum_{m=0}^{n-1} a_m e^{2imk\pi/n} = \sum_{0 \le m < n;(m,n)=1} e^{2imk\pi/n}$ which is the Ramanujan sum $c_n(k)$.

Therefore, we have shown:

Proposition. *The eigenvalues of the Cayley graph $\mathrm{Cay}(\mathbf{Z}_n, \mathbf{Z}_n^*)$ are the integers $c_n(k)$ for $0 \le k \le n-1$.*

5. Counting Generators in Cyclic Groups

In discussing heuristics on the Artin primitive root conjecture, one naturally looks at a positive integer a and needs to keep track of the index of the subgroup generated by a in $\mathbf{Z}_p^*$ for

various primes p (see [PM]). In this context, the following characteristic function plays a role and, once again, Ramanujan sums help in evaluating these functions. More precisely, we have:

Lemma. *Let G be a cyclic group of order n and $g \in G$. Then, for each divisor d of n,*

$$\sum_{h|d} c_h(O(G)/O(g)) = \begin{cases} d, & \text{if } d \text{ divides } O(G)/O(g) \\ 0, & \text{otherwise.} \end{cases}$$

Proof. We have already seen that

$$\sum_{h|d} c_h(k) = \sum_{h|d} c_h((k,d)).$$

We have also noted earlier that when $k|d$, we have

$$\sum_{h|d} c_h(k) = \begin{cases} d, & \text{if } k = d \\ 0, & \text{otherwise.} \end{cases}$$

Putting $k = O(G)/O(g)$, we have the assertion. □

6. Counting Cyclic Orbifolds

In this section, we discuss an interesting way to use Ramanujan sums to count the number of actions of a finite cyclic group as orientation-preserving automorphisms on a Riemann surface (see [VAL]). Such actions of a finite group G on a Riemann surface S of genus g correspond to epimorphisms of the fundamental group of the corresponding orbifold onto G. The fundamental group $\pi_1\Omega$ of an orbifold Ω can be described by $2g + r$ generators $x_1, y_1, \ldots, x_g, y_g, z_1, z_2, \ldots, z_r$ and relations

$$z_1 z_2 \ldots z_r \prod_{i=1}^{g} x_i y_i x_i^{-1} y_i^{-1} = 1, \quad z_i^{m_i} = 1 \; \forall \, i \le r,$$

for certain positive integers $1 < m_i \le |G|$.

To count epimorphisms from this group to a cyclic group $\mathbf{Z}_k$, one needs to simply look at the corresponding presentation of the finitely generated abelian group $\pi_1\Omega/[\pi_1\Omega, \pi_1\Omega]$. It is easy to prove that the number of order-preserving epimorphisms (that is, those epimorphisms which have torsion-free kernels) from $\pi_1\Omega(g, m_1, \ldots, m_r)$ to $\mathbf{Z}_k$ is:

$$m^{2g}\phi_{2g}(k/m)\frac{1}{M}\sum_{s=1}^{M} c_{m_1}(s)c_{m_2}(s)\ldots c_{m_r}(s),$$

where m = LCM of $m_1, \ldots, m_r$ divides M and, the above expression is independent of the choice of M (!).

Interestingly, the expression $\frac{1}{M}\sum_{s=1}^{M} c_{m_1}(s)c_{m_2}(s)\ldots c_{m_r}(s)$ on the right hand side above also counts the number of solutions to the congruence

$$x_1 + x_2 + \cdots + x_r \equiv 0 \bmod M,$$

with $GCD(x_i, M) = M/m_i$, where M is a multiple of the m_i's.

7. A Curious Application

Let $n > 1$ be odd. Fix $\zeta \in \Delta_n$ a primitive n-th root of unity. Writing the product $\prod_{i=1}^{(n-1)/2}(\zeta^i + \zeta^{-i}) = \sum_{k=1}^{n} M_k \zeta^k$, the number M_k counts the number of ways k can be written modulo n as $\pm 1 \pm 2 \cdots \pm (n-1)/2$. Also, for any divisor d of n,

$$\prod_{i=1}^{(n-1)/2}(\zeta^{di} + \zeta^{-di}) = \sum_{k=1}^{n} M_k \zeta^{dk} = \sum_{e|n} \sum_{(k,n)=n/e} M_k \zeta^{dk}$$

$$= \sum_{e|n} c_e(d) M_{n/e} \qquad (\heartsuit)$$

The left hand side can be evaluated independently to be $\pm 2^{(d-1)/2}$ where the sign is described as follows.

For any positive integer m, define $\left(\frac{2}{m}\right)$ to be 1 or -1 according as to whether the product $\prod a_p^{\alpha_p}$ is 1, and where α_p is 1 or -1 according as to whether 2 is a square modulo p or not and $\prod_p p^{\alpha_p} = m$.

Then, in ($\heartsuit$), the left hand side turns out to be $2^{(d-1)/2}\left(\frac{2}{n/d}\right)$.

The equations ($\heartsuit$) give a system of $d(n)$ linear equations, one for each divisor d of n. As we know how to invert the matrix of Ramanujan sums, we have the following beautiful result:

Theorem. *Let $n > 1$ be odd. Consider, for each $k \le n$, the number*

$$M_k = \left| \left\{ (\epsilon_1, \ldots, \epsilon_{d(n)}) : \epsilon_i = \pm 1, \sum_{i=1}^{(n-1)/2} i\epsilon_i \equiv k \bmod n \right\} \right|.$$

Then, we have $M_k = \frac{1}{n}\sum_{d|n} c_d(k) 2^{(\frac{n}{d}-1)/2}\left(\frac{2}{d}\right)$.

References

[BS] B. Sury, Cyclotomy and cyclotomic polynomials, *Resonance*, December (1999) 41–53.

[FGK] C. F. Fowler, S. R. Garcia and G. Karaali, Ramanujan sums as supercharacters, Ramanujan J., (in press) http://arxiv.org/abs/1201.1060.

[KS] W. Klotz and T. Sander, Some properties of unitary Cayley graphs, *The Electronic Journal of Combinatorics*, 14 (2007) #R45.

[PM] P. Moree, Artin primitive root conjecture – A survey, *Integers*, **12A** (2012) 1–100, #A13.

[SR] S. Ramanujan, On certain trigonometrical sums and their applications in the theory of numbers, *Trans. Cambridge Philos. Soc.*, **22** no. 13 (1918) 259–276.

[VAL] V. A. Liskovets, A multivariate arithmetic function of combinatorial and topological significance, *Integers*, **10** (2010) 155–177, #A12.

Problems and Solutions

Edited by Amritanshu Prasad

E-mail: problems@imsc.res.in

This section of the Newsletter contains problems contributed by the mathematical community. These problems range from mathematical brain-teasers through instructive exercises to challenging mathematical problems. Contributions are welcome from everyone, students, teachers, scientists and other maths enthusiasts. We are open to problems of all types. We only ask that they be reasonably original, and not more advanced than the MSc level. A cash prize of Rs. 500 will be given to those whose contributions are selected for publication. Please send solutions along with the problems. The solutions will be published in the next issue. Please send your contribution to problems@imsc.res.in with the word "**problems**" somewhere in the subject line. Please also send solutions to these problems (with the word "**solutions**" somewhere in the subject line). Selected solutions will be featured in the next issue of this Newsletter.

1. **D. Surya Ramanna, Harish-Chandra Research Institute, Allahabad.** Find all solutions to the equation $x^y = y^x$ in the positive integers.
2. **Thomas Moore, Bridgewater State University.** Squares $s_n = n^2$ and triangular numbers $t_n = \frac{n(n+1)}{2}$ are well known. The Jacobsthal numbers $j_n = \frac{2^n-(-1)^n}{3}$ for $n \geq 1$ are somewhat less well-known. Find a second degree polynomial with integer coefficients $f(x)$, such that, whenever the input s_n, t_n, or j_n, $n \geq 1$, the output is a triangular number.
3. **Kamalaskhya Mahatab, IMSc and Kannappan Sampath, ISI Bangalore.** Let $f(x)$ be a monic polynomial in $\mathbf{Z}[x]$ with a factorization

$$f(x) = \prod_{i=1}^{m} f_i(x),$$

with $f_1, \ldots, f_m$ are monic polynomials having no common factors. Let $g(x) \in \mathbb{Z}[x]$ be such that the remainder of $g(x)$ upon division by $f_i(x^n)$ is a polynomial in x^n for each i. Show that the residue of $g(x)$ upon division by $f(x)$ is a polynomial in x^n.
4. **Rahul Dattatraya Kitture, Bhaskaracharya Pratishthana, Pune.**
   (1) Prove that a group G can be written as a (set-theoretic) union of proper subgroups if and only if G is not cyclic.
   (2) Use (1) to prove that if G is a non-abelian group, then $G/Z(G)$ is not cyclic (here $Z(G)$ denotes the centre of G).
5. **K. N. Raghavan, IMSc.** Let n be a positive integer. Define d_n to be $(n+1)(n-1)$ if n is odd, and to be $(n+2)(n-2)$ if n is even; define e_n to be 4 or 0 accordingly as n is divisible by 3 or not. Show that the number of ways in which n can be written as a sum of three positive integers is $(d_n+e_n)/12$. (Can you write down an analogous expression for the number of ways of writing n as a sum of four positive integers?)

6. **K. N. Raghavan, IMSc.** Let n be a positive integer, $n \geq 2$. On the real two dimensional plane, consider the following two linear transformations: s is the reflection in the x-axis; and r rotation counter-clockwise by the angle $2\pi/n$.

$$sx = x \qquad rx = x\cos 2\pi/n + y \sin 2\pi/n$$
$$sy = -y \qquad ry = -x \sin 2\pi/n + y \cos 2\pi/n$$

Define a polynomial $f(x, y)$ to be *invariant* if $f(rx, ry) = f(sx, sy) = f(x, y)$. For example, the polynomial $f_0(x, y) = x^2 + y^2$ is invariant. (Geometrically, the two transformations s and r being respectively a reflection and a rotation, they preserve the inner product, which explains the invariance of $f_0(x, y)$.) Show that there exists a homogeneous invariant polynomial $f_1(x, y)$ of degree n such that, together with $f_0(x, y)$, it generates the ring of polynomial invariants (that is, any invariant polynomial is a polynomial with real coefficients in f_0 and f_1). For example, for the values 2 and 3 of n, we could take f_1 respectively to be $x^2 - y^2$ and $x^3 - 3xy^2$. Find an explicit closed formula for such an f_1 in terms of n. Show moreover that the expression as a polynomial in f_0 and f_1 of any invariant polynomial is unique.

7. **K. N. Ragahavan, IMSc.** A prime number p is called a *Fermat prime* if it is of the form $2^{2^k} + 1$ for some integer k. Prove or disprove the following: for any Fermat prime p with $k \geq 1$, the multiplicative group of units modulo p is generated by 3.

Solutions to Problems from the June Issue

1. **Abhishek Khetan, IIT Kharagpur.** Let $I_{2s} = \{1, 2, \ldots, 2s\}$. Let $\mathcal{F}$ be a collection of non-empty subsets of I_{2n} such that any two members of $\mathcal{F}$ have at least one element in common. Show that $|\mathcal{F}| \leq \binom{2s-1}{s-1}$.

First Solution. Define a function ϕ from $\mathcal{F}$ to the power set of I_{2s} by $\phi(A) = I_{2s} \backslash A$. Since any two members of $\mathcal{F}$ have at least one element in common, $\phi(A) \notin \mathcal{F}$. Thus $|\mathcal{F} \cup \phi(\mathcal{F})| = 2|\mathcal{F}| \leq \binom{2s}{s}$. Therefore $|\mathcal{F}| \leq \frac{1}{2}\binom{2s}{2} = \binom{2s-1}{s-1}$.

Second Solution. Partition $\mathcal{F}$ into two subsets:

$$\mathcal{F}_1 = \{A \in \mathcal{F} \mid 2s \in A\}, \quad \mathcal{F}_2 = \{A \in \mathcal{F} \mid 2s \notin A\},$$

and finally let $\mathcal{F}_2^* = \{B \cup \{2s\} \mid B \in \mathcal{J}_2\}$. If $A \in \mathcal{F}_2^* \cap F_1$, then $I_{2s} - A \in \mathcal{F}_2$, while $A \in \mathcal{F}_1$, so the disjoint sets A and $I_{2s} - A$ would both be in $\mathcal{F}$, contradicting the hypothesis. It follows that $\mathcal{F}_2^*$ is disjoint from $\mathcal{F}_1$. Now each element of $\mathcal{F}_2^* \cup \mathcal{F}_1$ contains $2s$. Therefore, $|\mathcal{F}_2^*| + |\mathcal{F}_1| \leq \binom{2s-1}{s-1}$. The result now follows from the fact that $|\mathcal{F}_2| = |\mathcal{F}_2^*|$.

2. **Tom Moore, Bridgewater State University.** Prove that the Diophantine equations

$$x^3 + y^3 = z^2, \quad x^4 + y^4 = z^3, \quad x^5 + y^5 = z^4$$

each have infinitely many positive integer solutions (x, y, z).

Solution. We found the following solutions for respective n values:

$$n = 3 : x = y = 2^{k+1} \quad \text{and} \quad z = 2^{3k+2}$$
$$n = 4 : x = y = 2^{3k+2} \quad \text{and} \quad z = 2^{4k+3}$$
$$n = 5 : x = y = 2^{4k+3} \quad \text{and} \quad z = 2^{5k+4},$$

and these suggested a general solution, for any positive integer $n \geq 3$, namely

$$x = y = 2^{(n-1)k+(n-2)} \quad \text{and} \quad z = 2^{nk+(n-1)}.$$

Checking the equation, we find that

$$\begin{aligned} x^n + y^n &= 2 \times 2^{n((n-1)k+(n-2))} \\ &= 2^{n(n-1)k+n(n-2)+1} \\ &= 2^{(n-1)(nk+(n-1))} \\ &= z^{n-1}. \end{aligned}$$

Solution received. Hari Kishan of D. N. College, Meerut has suggested $x = y = 2^{n-2}u^{n-1}$ and $z = 2^{n-1}u^n$ as solutions for $x^n + y^n = z^{n-1}$. For $x^3 + y^3 = z^2$, he has also suggested $x = u^4 + 8uv^3$, $y = -4u^3v + 4v^4$, and $z = u^6 - 20u^3v^3 - 8v^6$ as solutions.

3. **S. Kesavan, IMSc.** Let $I \subset \mathbf{R}$ be an interval and let $f : I \to \mathbf{R}$ be a continuous function which is not monotonic. Then, given any $\epsilon > 0$, show that there exist points $x(\epsilon)$ and $y(\epsilon)$ in I such that

$$x(\epsilon) \neq y(\epsilon), \quad |x(\epsilon) - y(\epsilon)| < \epsilon; \quad \text{and}$$
$$f(x(\epsilon)) = f(y(\epsilon)).$$

Solution. Since f is not monotonic, there exist distinct points $x_0 < y_0$ in I such that $f(x_0) = f(y_0)$. Let $T = y_0 - x_0$. Now consider

$$g(x) = f(x + T/2) - f(x)$$

defined on $[x_0, x_0 + T/2]$. Then either $g(x_0) = 0$ (in which case $g(x_0 + T/2) = 0$ as well) or $g(x_0) = -g(x_0 + T/2)$. In the latter case, by the intermediate value theorem, we get a point x' such that $g(x') = 0$ with $x_0 < x' < x_0 + T/2$. In either case we get a pair of points x_1 and y_1 such that $y_1 - x_1 = T/2$ and $f(x_1) = f(y_1)$. Iterating this procedure, we see that for any positive integer $n \geq 2$, there exist points x_n and $y_n - x_n = T/2^n$ such that $f(x_n) = f(y_n)$. This completes the proof.

Solution received. M. Suresh Kumar of NIT Surathkal sent in a correct solution to this problem.

4. **K. N. Raghavan, IMSc.** Given m distinct n-tuples of integers $p_1, \ldots, p_m$, and m integers $\alpha_1, \ldots, \alpha_m$, show that there exists a polynomial f in n variables (with rational coefficients) such that $f(p_1) = \alpha_1, \ldots, f(p_m) = \alpha_m$ and f takes integral values at all integer n-tuples.

Solution. We may assume $\alpha_1 = 1, \alpha_2 = \cdots = \alpha_m = 0$, for, if $f_1, \ldots, f_m$ are polynomials that take integer values on integer n-tuples and satisfy $f_j(p_k) = \delta_{jk}$ (Kronecker delta), then we need only set $f = \alpha_1 f_1 + \cdots + \alpha_m f_m$. We may assume p_1 to be the origin $(0, \ldots, 0)$, for, if g is a polynomial such that $g(0, \cdots, 0) = 1$ and $g(p_2 - p_1) = \cdots = g(p_m - p_1) = 0$, then we need only set $f(X) = g(X - p_1)$. Now choose N large enough to exceed moduli of all co-ordinates of $p_2, \ldots, p_m$. Set

$$f := \prod_{i=1}^{n} \binom{X_i + N}{N} \binom{-X_i + N}{N}$$

Here $\binom{A}{N}$ denotes the binomial coefficient, to be interpreted as

$$\frac{A(A-1)\ldots(A-N+1)}{N!} \quad \text{for any } A.$$

The polynomial $\binom{X+N}{N}$ takes integer values at integers, vanishes at $-N, -(N-1), \ldots, -1$, and is 1 at 0; and $\binom{X+N}{N}$ takes integer values at integers, vanishes at $1, 2, \ldots, N$, and is 1 at 0. Since each of the p_j has a non-zero co-ordinate in the range $[N, N]$, we see that $f(p_j) = 0$.

5. **B. Sury, ISI Bangalore.** If n is a natural number greater than 1 such that all its powers $n, n^2, n^3, n^4, \ldots$ have an odd number of digits, then n is a power of 100.

Solution. Clearly, powers of 100 have the asserted property and we need only prove the converse. If n has the mentioned property, then

$$10^{2k} \leq n < 10^{2k+1}$$

for some $k \geq 0$. Now

$$10^{4k} \leq n^2 < 10^{4k+2},$$

which actually means that

$$10^{4k} \leq n^2 < 10^{4k+1},$$

because n^2 has an odd number of digits. Similarly,

$$10^{2^d k} \leq n^{2^{d-1}} < 10^{2^d+1}.$$

Thus $10^{2k} \leq n < 10^{2k+1/2^{d-1}}$ for all d which gives $n = 10^{2k}$.

6. **B. Sury, ISI Bangalore.** Find all pairs of primes p, q, whose sum is a power of their difference.

Solution. Let $p + q = (p - q)^r$ where $p > q$ are primes. If l is a prime dividing $p - q$, then $p + q \equiv 2q \equiv 0 \mod l$ (the last because $p + q = (p - q)^r$). So, $l = 2$, or $l = q$. If $l = q$, then $p = l = q$, a contradiction.

Therefore $l = 2$, and p, q are odd primes. So $p - q = 2^k$ for some $k \geq 1$. Hence $p + q = 2^k + 2q = (p - q)^r = 2^{kr}$. So $q = 2^{kr-1} - 2^{k-1} = 2^{k-1}(2^{k(r-1)} - 1)$. As q is an odd prime, this gives $k - 1 = 0$, which gives $q = 2^{r-1} - 1$ and $p = q + 2 = 2^{r-1} + 1$. The fact that q is prime implies that $r - 1$ is prime. If $r - 1 = 2$, we get the solution $r = 3$, $q = 3$ and $p = 5$; that is

$$5 + 3 = (5 - 3)^3. \qquad (*)$$

If $r - 1$ is an odd prime, then $p = 2^{r-1} + 1$ is a multiple of $2 + 1$, and is bigger than 3, and hence is not a prime. So (*) gives the unique solution.

Solution received. Aditi Phadke of Nowrosjee Wadia college sent in a correct solution to this problem by a different method.

7. **Amritanshu Prasad, IMSc.** Show that the probability that a monic polynomial of degree n in with coefficients in a

finite field of order q is square-free is $1-q^{-1}$ for all integers $n > 1$.

Solution. Since there are q^n monic polynomials of degree n, we need to show that for $n > 1$, there are $q^n - q^{n-1}$ square-free monic polynomials.

By the unique factorization theorem for polynomials over a field, every monic polynomial can be uniquely written as the product of a monic square and a monic square-free polynomial. Therefore if $c_n(q)$ is the number of square-free polynomials of degree n then

$$q^n = \sum_{r=0}^{\lfloor n/2 \rfloor} q^{2r} c_{n-2r}(q),$$

whence

$$c_n(q) = q^n - \sum_{r=1}^{\lfloor n/2 \rfloor} q^{2r} c_{n-2r}(q). \qquad (\dagger)$$

We now proceed inductively: we have the base cases $c_0(q) = 1$, $c_1(q) = q$ (since all monic polynomials of degree 0 and 1 are square-free). Using (†) we find that

$$c_2(q) = q^2 - q \quad \text{and} \quad c_3(q) = q^3 - q^2.$$

We now proceed by induction. If n is even, (†) gives

$$c_n(q) = q^n - c_{n-2}(q)q - c_{n-4}(q)q^2 - \cdots - c_2(q)q^{\lfloor n/2 \rfloor - 1} - c_0(q)q^{\lfloor n/2 \rfloor}.$$

If we assume the result to be true for all $m < n$, then the above identity becomes

$$c_n(q) = q^n - (q^{n-2} - q^{n-3})q - (q^{n-4} - q^{n-5})q^2 - \cdots - (q^2 - q)q^{\lfloor n/2 \rfloor - 1} - q^{\lfloor n/2 \rfloor},$$

which telescopes to $q^n - q^{n-1}$. A similar proof works for odd n.

Indo-French Centre for Applied Mathematics (IFCAM)

Indian Institute of Science, Bangalore

Visitors Programme

The Indo-French Centre for Applied Mathematics (IFCAM) has been jointly set up by the Indian and French Governments at the Indian Institute of Science, Bangalore as an international joint research unit. IFCAM is designed as a platform for cooperation in mathematical sciences with the primary focus being the area of applied mathematics.

IFCAM has funds to support visits of Indian researchers, particularly from Universities and Colleges, working in applied mathematics (interpreted broadly to include mathematical aspects of engineering, physics, biology etc). Visitors can be hosted either at IFCAM, Indian Institute of Science, Bangalore or at a neighboring research institution (subject to consent of the institution). Visits can range from 1 month to 3 months and should aim to initiate or continue a research collaboration with a faculty member at the host institute. Interested researchers should apply online through the website given below. All visits should be completed by March 31, 2014. Selected visitors would be paid TA/DA for the duration of the visit. Further details on all of the above along with the application form can be obtained from:

`http://www.math.iisc.ernet.in/~ifcam/visitors.html`

Director:

Indo-French Centre for Applied Mathematics
Department of Mathematics, Indian Institute of Science
Bangalore 560 012, India

Tel: +91-80-2360 0365 | Fax: +91-80-2360 0365

E-mail: `ifcam@math.iisc.ernet.in` | `http://www.math.iisc.ernet.in/~ifcam/`

International Symposium on Complex Analysis and Conformal Geometry (ISCACG 2013)

28–30 December, 2013

Organizing Institution: Indian Institute of Technology Indore.

Aim: This symposium is mainly aimed at young researchers from all over the country who are interested in research in the following areas of Complex Analysis of current relevance: univalent harmonic mappings, hyperbolic geometry and functions spaces. It will put special emphasis on exposure

of Ph.D. students and post-doctoral fellows from India to the latest trends. In particular, young Indian research scholars will be able to learn about the recent developments in the above areas, new avenues in current research, and their connections to related fields. It also aims to bring ideas and inspiration to their ongoing research work, and to foster conversations between them and the senior researchers participating in the programme.

Further information on the symposium will be available shortly at www.iiti.ac.in/∼iscacg2013

Contact Address:

Dr. Swadesh Kumar Sahoo
Convener, ISCACG 2013
Assistant Professor
Indian Institute of Technology Indore
M-Block, IET-DAVV Campus
Khandwa Road, Indore 452 017

Call for Applications BMS Dirichlet Postdoctoral Fellowship

The Berlin Mathematical School (BMS) invites applications for the Dirichlet Postdoctoral Fellowship starting in the fall of 2014. This two-year position is open to promising young mathematicians holding a PhD who want to pursue their own research in any of the fields of mathematics represented in Berlin. The competitive full-year salary includes health insurance. Fellows are expected to teach one course per semester, typically in English and at the graduate level.

Completed applications are due by 1 December 2013, and should be submitted online at the BMS website:

http://www.math-berlin.de/about-bms/dirichlet-fellowship

Applications from all well-qualified individuals, especially women, are highly encouraged. The Berlin Mathematical School (BMS) is a joint graduate school of the mathematics departments of the three major Berlin universities: Freie Universität (FU), Humboldt-Universität (HU) and Technische Universität (TU). The BMS has been funded under the German "Excellence Initiative" since October 2006.

Contact:

Phone: +49 30 314 78651
E-mail: office@math-berlin.de
Web: http://www.math-berlin.de

Details of Workshop/Conferences in India

For details regarding Advanced Training in Mathematics Schools
Visit: http://www.atmschools.org/

Name: IWM2013-Teachers Training Programme
Date: December 23–28, 2013
Location: Department of Mathematics, Mumbai University
Visit: https://sites.google.com/site/iwm2013ttp/

Name: International Conference on Recent Advances in Statistics and Their Applications
Date: December 26–28, 2013
Location: Dr. BabasahebAmbedkarMarathwada University, Aurangabad
Visit: http://www.bamu.ac.in/icrastat2013/

Name: International Conference on Mathematics and Computing – 2013
Date: December 26–29, 2013

Location: Haldia Institute of Technology, Haldia, West Bengal
Visit: http://hithaldia.in/icmc2013/

Name: 22nd National and 11th ISHMT ASME Heat and Mass transfer Conference
Date: December 28–31, 2013
Location: IIT Kharagpur, Kharagpur
Visit: http://ishmt2013iitkgp.in/

Name: 42nd Annual Conference of OMS & International Conference on Industrial Mathematics and Scientific Computing
Date: January 4–5, 2014
Location: KIIT University, Bhubaneswar, Odisha.
Visit: http://icimsc2014.org/

Name: 8th International conference on matrix analytic methods in stochastic models
Date: January 6–10, 2014
Location: National Institute of Technology Calicut (NITC), Kerala
Visit: http://mam8.nitc.ac.in/

Name: International Conference on Recent Advances in Mathematics (ICRAM 2014)
Date: January 20–23, 2014
Location: Rashtrasant Tukodoji Maharaj Nagpur University, Nagpur
Visit: http://icram2014.com/

For more details and updates regarding workshop/conferences in India please
Visit: http://www.conference-service.com/conferences/in/

Details of Workshop/Conferences in Abroad

For details regarding ICTP (International Centre for Theoretical Physics)
Visit: http://www.ictp.it/

Name: 3rd Annual International Conference on Computational Mathematics, Computational Geometry & Statistics (CMCGS 2014)
Date: February 3–4, 2014
Location: Hotel Fort Canning, 11 Canning Walk, Singapore, Singapore 17881.
Visit: http://www.mathsstat.org/

Name: Introductory Workshop: Model Theory, Arithmetic Geometry and Number Theory
Date: February 3–7, 2014
Location: Mathematical Sciences Research Institute, Berkeley, California.
Visit: http://www.msri.org/workshops/688

Name: ICERM Semester Program on “Network Science and Graph Algorithms”
Date: February 3–May 9, 2014

Location: ICERM, Providence, Rhode Island
Visit: http://icerm.brown.edu/sp-s14

Name: Function Theory on Infinite Dimensional Spaces XIII
Date: February 4–7, 2014
Location: ICMAT, Campus de Cantoblanco, Madrid, Spain
Visit: http://www.icmat.es/congresos/2014/ftida/

Name: Connections for Women: Model Theory and its interactions with number theory and arithmetic geometry
Date: February 10–11, 2014
Location: Mathematical Sciences Research Institute, Berkeley, California
Visit: http://www.msri.org/web/msri/scientific/workshops/all-workshops/show/-/event/Wm9548

Name: ICERM Workshop: Semidefinite Programming and Graph Algorithms
Date: February 10–14, 2014
Location: ICERM, Providence, Rhode Island.
Visit: http://icerm.brown.edu/sp-s14-w1

Name: Translating Cancer Data and Models to Clinical Practice
Date: February 10–14, 2014
Location: Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California
Visit: http://www.ipam.ucla.edu/programs/cdm2014/

Name: Higher Structures in Algebraic Analysis
Date: February 10–21, 2014
Location: University of Padova, Department of Mathematics, Padova, Italy
Visit: http://events.math.unipd.it/hsaa/

Name: Hot Topics: Perfectoid Spaces and their Applications
Date: February 17–21, 2014
Location: Mathematical Sciences Research Institute, Berkeley, California
Visit: http://www.msri.org/workshops/731

Name: Stochastic Gradient Methods
Date: February 24–28, 2014
Location: Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California
Visit: http://www.ipam.ucla.edu/programs/sgm2014/

Name: XIX SIMMAC – International Symposium on Mathematical Methods Applied to the Sciences
Date: February 25–28, 2014
Location: University of Costa Rica, San Jose, Costa Rica
Visit: http://www.cimpa.ucr.ac.cr/simmac/en/

Name: AIM Workshop: Postcritically finite maps in complex and arithmetic dynamics
Date: March 3–7, 2014

Location: American Institute of Mathematics, Palo Alto, California
Visit: http://www.aimath.org/ARCC/workshops/finitedynamics.html

Name: 11th German Probability and Statistics Days 2014 – Ulmer Stochastik-Tage
Date: March 4–7, 2014
Location: University Ulm, Ulm, Germany
Visit: http://www.gpsd-ulm2014.de

Name: International Workshop on Discrete Structures (IWODS)
Date: March 5–7, 2014
Location: Centre for Advanced Mathematics and Physics, National University of Sciences and Technology, H-12 Islamabad, Pakistan
Visit: http://www.camp.nust.edu.pk/IWODS2014/

Name: School and Workshop on Classification and Regression Trees
Date: March 10–26, 2014
Location: Institute for Mathematical Sciences, National University of Singapore, Singapore
Visit: http://www2.ims.nus.edu.sg/Programs/014swclass/index.php

Name: Algebraic Techniques for Combinatorial and Computational Geometry
Date: March 10–June 13, 2014
Location: Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California
Visit: http://www.ipam.ucla.edu/programs/ccg2014

Name: Algebraic Techniques for Combinatorial and Computational Geometry: Tutorials
Date: March 11–14, 2014
Location: Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California
Visit: http://www.ipam.ucla.edu/programs/ccgtut/

Name: IAENG International Conference on Operations Research 2014
Date: March 12–14, 2014
Location: Hong Kong, China
Visit: http://www.iaeng.org/IMECS2014/ICOR2014.html

Name: 48th Annual Spring Topology and Dynamical Systems Conference
Date: March 13–15, 2014
Location: University of Richmond, Richmond, Virginia
Visit: http://math.richmond.edu/resources/topology-conference/index.html

Name: Representation Theory and Geometry of Reductive Groups
Date: March 14–28, 2014
Location: KlosterHeiligkreuztal, a Monastary in Germany, Altheim, Germany
Visit: http://www2.math.uni-paderborn.de/konferenzen/conferencespring-school.html

Name: ICERM Workshop: Stochastic Graph Models
Date: March 17–21, 2014

Location: ICERM, Providence, Rhode Island
Visit: http://icerm.brown.edu/sp-s14-w2

Name: 2nd Annual International Conference on Architecture and Civil Engineering (ACE 2014)
Date: March 24–25, 2014
Location: Hotel Fort Canning, 11 Canning Walk, Singapore, Singapore 17881
Visit: http://www.ace-conference.org/

Name: Combinatorial Geometry Problems at the Algebraic Interface
Date: March 24–28, 2014
Location: Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California
Visit: http://www.ipam.ucla.edu/programs/ccgws1/

Name: Mathematical, Statistical and Computational Aspects of the New Science of Metagenomics
Date: March 24–April 17, 2014
Location: Isaac Newton Institute for Mathematical Sciences, Cambridge, United Kingdom
Visit: http://www.newton.ac.uk/programmes/MTG/index.html

Name: 38th Annual SIAM Southeastern Atlantic Section (SEAS) Conference
Date: March 28–30, 2014
Location: Florida Institute of Technology, Melbourne, Florida
Visit: http://my.fit.edu/∼abdulla/SIAMSEAS-2014

Name: SIAM Conference on Uncertainty Quantification (UQ14)
Date: March 31–April 3, 2014
Location: Hyatt Regency Savannah, Savannah, Georgia, USA
Visit: http://www.siam.org/meetings/uq14/

Name: Ischia Group Theory 2014
Date: April 1–5, 2014
Location: Grand Hotel delleTerme Re Ferdinando, Ischia, Naples, Italy
Visit: http://www.dipmat.unisa.it/ischiagrouptheory/

Name: 13th New Mexico Analysis Seminar
Date: April 3–4, 2014
Location: University of New Mexico, Albuquerque, New Mexico
Visit: http://www.math.unm.edu/conferences/13thAnalysis/

Name: AIM Workshop: The many facets of the Maslov index
Date: April 7–11, 2014
Location: American Institute of Mathematics, Palo Alto, California
Visit: http://www.aimath.org/ARCC/workshops/maslov.html

Name: ICERM Workshop: Electrical Flows, Graph Laplacians, and Algorithms: Spectral Graph Theory and Beyond
Date: April 7–11, 2014

Location: ICERM, Providence, Rhode Island
Visit: http://icerm.brown.edu/sp-s14-w3

Name: Reimagining the Foundations of Algebraic Topology
Date: April 7–11, 2014
Location: Mathematical Sciences Research Institute, Berkeley, California
Visit: http://www.msri.org/web/msri/scientific/workshops/programmatic-workshops/show/-/event/Wm9550

Name: Tools from Algebraic Geometry
Date: April 7–11, 2014
Location: Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California
Visit: http://www.ipam.ucla.edu/programs/ccgws2/

Name: Advanced Monte Carlo Methods for Complex Inference Problems
Date: April 22–May 16, 2014
Location: Isaac Newton Institute for Mathematical Sciences, Cambridge, United Kingdom
Visit: http://www.newton.ac.uk/programmes/MCM/index.html

Name: International arab conference on mathematics and computations
Date: April 23–25, 2014
Location: Zarqa University, Zarqa, Jordan
Visit: http://www.iacmc.org

Name: AIM Workshop: Exact crossing numbers
Date: April 28–May 2, 2014
Location: American Institute of Mathematics, Palo Alto, California
Visit: http://www.aimath.org/ARCC/workshops/exactcrossing.html