This is the published version:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30008212

Reproduced with the kind permission of the copyright owner.

Copyright: 2007, Australian Association of Mathematics Teachers Inc.
Mathematicians, mathematics and mathematics teaching: Personal perspectives

Susie Groves
Deakin University

How can we enrich the mathematical experiences of our students? This paper attempts to explore ways in which a consideration of the work of contemporary mathematicians, and the applications of contemporary mathematics, can be used to enhance the learning and teaching of mathematics. It also looks briefly at Hanna Neumann’s contribution to mathematics education.

Introduction

Mathematics is sometimes thought of as a great entity, like a tree, branching off into several large chunks of mathematics which themselves branch off into specialised fields, until the very ends of the tree are reached, where the blossoms and the fruit are found. (Tao, 1992, p. 65)

The tree and branch analogy for mathematics and its disciplines is probably a familiar one for most people, even in the wider community. However, I suspect few people think about the blossoms and the fruit — the place where new mathematics grows — and that even fewer think about the people who create this new mathematics — the mathematicians.

At the time when I was asked to choose a title for this Hanna Neumann Memorial Lecture, Terence Tao had just been awarded the Fields Medal — the equivalent of the Nobel Prize in mathematics. At about the same time, one of my doctoral students, Linda Darby, was telling me that one of the major differences she had found, in her work with teachers of mathematics and science, was the much more frequent use of narrative in science teaching than in mathematics (Darby, 2005). Yet, there are so many stories to tell — not just the ones from the history of mathematics books — and so many ways to use them.

In this paper, I will try to use some of these stories to illustrate what I believe are some important ways in which mathematics teaching can be enhanced by their use.

I am honoured and delighted to have been asked to present this Hanna Neumann Memorial Lecture. While Hanna needs no introduction, and I am sure someone else will introduce her life and work at the lecture, I will, nevertheless, begin by saying a little about Hanna herself.

Hanna Neumann

Hanna Neumann was born in Berlin in February 1914. She lived a remarkably full and prolific life until her unexpected death in November 1971 while on a lecture tour in Canada. Hanna married Bernhard Neumann in Cardiff in 1939. She had left Germany in

* Invited paper
1938 to join Bernhard, who had left Germany five years earlier to escape the Nazis. Together they had five children, two of whom, Peter and Walter, also became well known mathematicians, while two others, Daniel and Barbara, completed degrees in mathematics, with Barbara also teaching mathematics.

Hanna completed her D Phil at Oxford in 1943, writing her thesis largely by candlelight in a caravan. She was often seen transporting her two small children around Oxford in a side-car attached to her bicycle. After an active academic life in Britain, which unfortunately meant that she and Bernhard frequently needed to live apart, Hanna and Bernhard were both offered prestigious positions at the Australian National University (ANU). Bernhard was asked to set up and head a research department in mathematics, while Hanna’s position, which she took up in 1963 a year after Bernhard came to Australia, soon became a Chair in Pure Mathematics and head of the department of Pure Mathematics in the undergraduate part of the university.

I was fortunate to know both Hanna and Bernhard from early 1970 when I started as a doctoral student in pure mathematics at the Australian National University, under the supervision of M. F. (Mike) Newman and Laci Kovacs. In their comprehensive obituary, which pays tribute to Hanna’s life and work, Newman and Wall (1974) describe Hanna as “enthusiastic, inspiring, energetic, firm, tactful, sympathetic efficient, patient, shrewd, humble, peace-loving, courageous, gracious…” (p. 1). For me, each of these words evokes vivid memories of Hanna.

However, this is not intended to be an historical or personal account of Hanna’s life. Rather, I would like to explore, however briefly, some of her views about, and contributions to, mathematics education. Newman and Wall (1974) capture not only the joy that Hanna found in mathematics, but also her frustration with curriculum and pedagogy that failed to reveal what she saw as the nature of mathematics — especially the fact that “doing and thinking mathematics can be joyous human activities” (p. 11) — and its many applications to a wide range of areas in everyday and professional life.

While still in Britain, Hanna attempted to introduce more modern pure mathematics to her university course, which she described rather scathingly as spending so much time “on enabling students to solve problems — or perhaps: so much more care is taken to turn out students not worried by an integral or a differential equation” (cited in Newman & Wall, 1974, p. 6). Almost 60 years later, this complaint could perhaps still be made of many mathematics courses in Australian schools and universities!

During her time in Manchester from 1958 to 1963, Hanna had the opportunity to develop and teach courses more in tune with her view of what mathematics is really about. She was able to use concrete examples to help students access abstract ideas in her undergraduate algebra courses, as well as illustrate to students that areas of mathematics, other than calculus, have applications in real life.

In Australia, Hanna soon became involved in secondary school mathematics. She gave lectures and in-service courses for teachers in and around Canberra. She was active in the Canberra Mathematical Association, critiquing the proposed new syllabus and working hard to persuade the community that mathematics is not something to be feared. Her involvement led her to be elected as one of the foundation Vice-Presidents of the Australian Association of Mathematics Teachers (AAMT) in 1966, the first President of AAMT being Bernhard Neumann. She gave lectures to school students in Canberra and was an enthusiastic supporter and contributor to the ANU-AAMT National Summer School for talented high school students, which was started in 1969.

Hanna published over 30 papers in mathematics, as well as a highly regarded pamphlet on probability for teachers (Neumann, 1996) and an article on teaching
undergraduate students, published after her death in the Australian Mathematics Teacher (Neumann, 1973).

In my opinion, Hanna’s life and work show that mathematicians and mathematics teachers can work together productively to enhance the teaching of mathematics in schools — something that is sometimes obscured by events such as the recent US “Maths Wars”. Hanna’s vision of school mathematics, and mathematics in general, was that of a joyful activity (which is necessarily done by real people), rather than the rote learning of rules and procedures. She had a vision of contemporary mathematics having a significant place in the curriculum, together with the need to show the wide range of applications of pure mathematics to our students. Even now, 35 years after her death, the realisation of Hanna’s vision is as important a goal as it was in the late 1960s.

We will now look very briefly at the life and work of another mathematician, Cheryl Praeger, who not only had strong connections with Hanna Neumann, but whose work allows us an opportunity to explore a relatively simple application of pure mathematics.

Cheryl Praeger

Cheryl Praeger was born in Toowoomba in 1948 to parents who, having come from poor backgrounds with no chance of going to university, encouraged their children to do so (MacTutor History of Mathematics archive, 2006). While completing her BSc at the University of Queensland, Cheryl spent eight weeks at the Australian National University on a summer research scholarship (after her third year), working on a problem suggested to her by Bernhard Neumann, which resulted in a published paper (Praeger, 1970). After completing her undergraduate course, Cheryl went to Oxford on a Commonwealth Scholarship to study for her doctorate in finite permutation groups under the supervision of Peter Neumann, Hanna and Bernhard’s son. In 1973, Cheryl was appointed to a three year postdoctoral fellowship at ANU, with her time there overlapping briefly with mine as a doctoral student.

Cheryl has been at the University of Western Australia since 1976, where she has been Professor of Mathematics since 1983. She is a Fellow of the Australian Academy of Science, former president of the Australian Mathematical Society, and a member of the Order of Australia. Like Hanna Neumann, Cheryl exudes joy in her work as a mathematician, looks for the applications of pure mathematics, and takes a keen interest in mathematics education. Her work on combinatorial designs led her to explore their application to experimental layouts for agricultural experiments, in order to help statisticians understand the symmetry groups involved. She has over 300 publications, including four books, over 250 research papers in mathematics, and a number of articles about mathematics education or for teachers.

One of Cheryl’s most popular lecture topics, aimed at school level, has been on the mathematics of weaving. One of her three papers on this topic is published as part of The Hanna Neumann Memorial Lectures at ICME 5 (see Praeger, 1986). In this paper, Cheryl describes how several problems in weaving materials can be solved using mathematics. She firstly explains how a real woven fabric can be modelled with the use of binary matrices representing a fundamental block (or smallest repeating block in the pattern). A problem in weaving is to determine which patterns produce fabrics that hang together — that is, which patterns produce fabrics where the warp and weft threads do not have subsets that can completely lift off the fabric. It can be shown that fabrics will not hang together exactly when the binary matrix representing the fundamental block of the pattern can be transformed by rearranging its rows and columns, in such a way, as to get a matrix of the form
\[ \begin{pmatrix} X & 0 \\ J & Y \end{pmatrix} \]

where 0 is a matrix with all entries zero, and J is a matrix with all entries one.

However, finding out whether or not the matrix representing the fundamental block of the pattern can be transformed in such a way would take far too long, when the size of the matrix is large. In her paper, Praeger describes different algorithms that can be used to decide whether or not woven fabrics represented by a particular fundamental block would hang together, as well as the way in which the factorisation of binary matrices can be used to set up a loom to weave the fabric, represented by such a fundamental block.

Applications such as these go along way towards answering the perennial student question of "Why are we learning this?" even though we do not expect every student to become a weaver of fabric!

This focus on the applications of pure mathematics is also taken up by another Australian mathematician of world renown, Terence Tao.

**Terence Tao**

Readers of most Australian newspapers would be aware that in August 2006 Terence Tao became the first Australian mathematician to be awarded the Fields Medal (see, for example, Cauchi, 2006). In further recognition of his outstanding work, Terence Tao was also named South Australia's Australian of the Year for 2006 (see, for example, Novak, 2006) and elected as a Fellow of the Royal Society in May 2007.

Aged 31, Terence Tao has been a full professor of mathematics at UCLA since 2000, and has long been regarded as likely to win the Fields Medal, which is awarded every four years (UCLA College, 2005). He has over 80 published papers and has worked, with more than 30 collaborators, on an amazingly wide range of mathematical problems.

One of the highlights of Terence Tao’s work has been his work with Ben Green on a classical question regarding prime numbers (see Ross & Polster, 2007). Tao is also credited with having extraordinary abilities in assembling and managing world-class teams of mathematicians to work on problems.

Terence Tao was born in Adelaide in 1975. In April 1983, when Terence was seven years old, the Adelaide Advertiser carried an article entitled *Tiny Terence, 7, is High School Whiz* (cited in Clements, 1984). At that time, Dr M. A. (Ken) Clements, who is now at Illinois State University, was undertaking a bible college course in Adelaide after having “given up” mathematics education following eight years in the Faculty of Education at Monash University, and many years as a teacher of secondary school mathematics. Nevertheless, when asked by Terence’s father to assess his son’s mathematical abilities, Ken, who had a long-standing interested in mathematically gifted students, found he could not refuse. This began a relatively long association between Terence and Ken. Terence, at age seven, was exceptionally gifted. He was spending the equivalent of two days a week at high school studying Year 11 mathematics and physics, and the rest of his time at his local primary school, being happy and well accepted in both places. In 1986, at age ten, Terence became the youngest participant in the International Mathematical Olympiads, winning a bronze, silver and gold medal in 1986, 1987 and 1988 respectively. He graduated with a bachelor and master’s degree from Flinders University at age 17 and a Ph D from Princeton at age 20, joining the UCLA Faculty that year.
After several years working as a missionary in India, Ken Clements (whom I have known for over 30 years) returned to Australia and joined Deakin University. In 1992, Terence Tao published his first book (Tao, 1992), a monograph commissioned by Ken Clements and Nerida Ellerton to form part of the study materials for the Deakin University unit *Teaching Mathematics Through a Problem Solving Approach*. The manuscript for this book was prepared in early 1991, when Terence was 15 years old. The monograph, which was used for a number of years by various Deakin staff, including myself, in a number of units about problem solving, was reprinted by Oxford University Press in 2006.

Regarding the applications of pure mathematics, Terence Tao has this to say:

> Mathematicians often work on pure problems that may not have applications for 20 years — and then a physicist or computer scientist or engineer has a real-life problem that requires the solution of a mathematical problem, and finds that someone already solved it 20 years ago... When Einstein developed his theory of relativity, he needed a theory of curved space. Einstein found that a mathematician had devised exactly the theory he needed more than 30 years earlier.
> 
> (UCLA College, 2005)

It is easy to believe that pure mathematics in general, and number theory in particular, are all very well as genteel pastimes, but have no use in the real world. In fact, nothing could be further from the truth. In the chapter *Examples in number theory*, Tao (1992) writes: “Basic number theory is a pleasant backwater of mathematics. But the applications that stem from the basic concepts of integers and divisibility are amazingly diverse and powerful” (p. 8). To illustrate this, we will take a tiny glimpse at the way in which mathematics has been used in recent history in the design and breaking of codes.

**Public-key cryptography**

Codes are used when we want to transmit (secret) messages which are in danger of being intercepted. Alan Turing, who was one of the most influential figures in the development of the electronic computer, was also the presiding mathematical genius at Bletchley Park during World War II where he, more than any other person, made possible the breaking of the Enigma codes. The operations of the mathematicians, linguists and other scientists at Bletchley Park formed the basis, some years ago, for a spellbinding British documentary series *The Secret War*, which some of you may have seen, when it was shown on ABC television.

It is easy to think of codes and code breaking as only being of use in war-time, but codes are also essential when we want to store and transmit electronic data — something which happens now in every facet of life, from banking to telecommunications, to the storage of personal information on citizens, to purchasing products on eBay, all of which we want to make sure is secure. (You will all have seen messages regarding the security status of web pages you are viewing — for example, alerting you that you are leaving a page that supports encryption.)

In traditional coding systems, the key to *encode* a message can also be used to *decode* it. Therefore, this (single) key must be kept secret and only made available to people with whom you are communicating — hence, the importance of breaking codes such as the Enigma code in World War II.

In everyday modern life, however, there is such a vast amount of data handling which involves the need for security, that it certainly would not be practicable to use
traditional codes, which, apart from anything else, need the key to be agreed on between
the users of the code.

It turns out that the ease with which primes can be multiplied together, compared
with the enormous difficulty of factorising a number when we do not know its factors,
can be used to create a new type of coding or encryption which is called public-key
cryptography.

In public-key cryptography, the key for decoding a message cannot be deduced from
the key for encoding it — at least not in a feasible amount of time. This allows people
to send secure messages, electronically, to a destination which can publicly advertise
the encoding key — hence, the name public-key cryptography. All of these systems
depend on the fact that, while it is theoretically possible to deduce the decoding key
from the encoding key (for example, as a last resort, by encoding every possible
message of the same length as the one intercepted and seeing which message encodes to
the message received), it is not feasible to do so in the time available.

A useful metaphor is to think about a traditional cryptosystem as a safe with a
combination lock that, when you know the combination, allows you to both lock and
unlock the safe, while in a public-key system the safe has two separate combination
locks: one that locks the safe and another that unlocks it. Such codes are also sometimes
called trapdoor codes: one where it is very easy to do something (encode a message)
but very hard to undo it (decode the message).

One of the earliest public-key cryptosystems, the so-called RSA system, was devised
by Ted Rivest, Adi Shamir and Leonard Adleman (see, for example, Hellman, 1978 for
a description of several systems, including RSA). The RSA system depends on the
difficulty of factorising large numbers, as well as making use of modular arithmetic,
and some fairly elementary results from number theory. The system can be described,
briefly, as follows:

Setting up the system

Select two large primes, \( p \) and \( q \), each about 100 digits long. (These primes will remain
secret.)

Let \( n = p \times q \). (The number \( n \) will be made public, but knowing \( n \) will not make it
possible for you to determine \( p \) and \( q \) because of the difficulty of factorising a number.)

The Euler function \( \varphi(n) = (p - 1)(q - 1) \) is the number of integers between 1 and \( n \)
that are relatively prime to \( n \); that is, the number of integers whose only common factor
with \( n \) is 1. The Euler function \( \varphi(n) \) has the property that for any integer \( a \) between 0
and \( n - 1 \),

\[
a^{1 + k \cdot \varphi(n)} \equiv a \mod n.
\]

Choose a random positive integer \( E < \varphi(n) \), such that \( E \) is relatively prime to \( \varphi(n) \).

\( E \), like \( n \), will be made public: together \( n \) and \( E \) make up the public key.

Since the person setting up the code knows the secret primes \( p \) and \( q \), they also know
the value of \( \varphi(n) = (p - 1)(q - 1) \), but this remains a secret for the public. So, for the
person setting up the code, it is easy to find the inverse of \( E \) modulo \( \varphi(n) \); that is, the
number \( D \) such that

\[
D \cdot E = 1 \mod \varphi(n),
\]

that is, the number \( D \) such that

\[
D \cdot E = 1 + k \cdot \varphi(n)
\]

for some integer \( k \).
This number \( D \) also remains secret.

Summing up this stage, we have the following:
- secret: \( p, q, \varphi(n), D \);
- public: \( n, E \).

**Encryption**

The first step is to represent any message as a sequence of integers. (There are many simple ways to do this, but we will not discuss them here.) Each message then needs to be split up into blocks of digits, each being a number less than \( n \). Each block is then encoded separately.

Let \( P \) be a block in our “message”; that is, an integer between 0 and \( n - 1 \).

Now let

\[
C = P^E \mod n
\]

that is, we raise \( P \) to the power \( E \) and find the remainder when you divide by \( n \).

So, \( C \) is the encrypted or coded message corresponding to the original message \( P \), and \( C \) is the message that is transmitted, by whatever (possibly insecure) means we are using.

**Decryption**

To decode the message \( C \), we find \( P \) by calculating

\[
P = C^D \mod n.
\]

Why does this work? Since we have

\[
C = P^E \mod n,
\]

we get

\[
C^D \mod n = P^{E.D} \mod n = P^{1 + k.\varphi(n)} \mod n = P \mod n, \text{ since } 0 < P < n.
\]

**Does RSA work?**

When the RSA code was developed, it was estimated that it would take a million years to factor the 200 digit number \( n = p \times q \), using the fastest known (computer) algorithms known at the time. Of course, computers get faster and faster so methods, such as these, produce codes that fail, in time. New cryptosystems are constantly being developed to meet this important need for secure storage and transmission of digital information. It is perhaps interesting to note that, unlike the way we usually think of mathematics as representing facts and certainty, it is theoretically possible to break such cryptosystems, but they are, for a time anyway, practically intractable.

Public-key cryptography has led to a dramatic upsurge of interest in techniques for factorisation of numbers, and number theory in general.

While the explanation given here appears difficult, it is possible to illustrate it relatively easily using small numbers; e.g., by choosing \( p = 5, q = 11, E = 7 \) and \( P = 2 \) (see Hellman, 1978, p. 27 for more details). Doing such worked examples is possible in
secondary mathematics classes, but even primary children can be exposed to some of the general principles involved and the fact that factorisation, and the use of divisibility tests, have significant contemporary applications.

We will conclude our examples of the applications of mathematics by considering the role of mathematics in one branch of art and design.

**M. C. Escher and George Pólya**

The famous Dutch artist M. C. Escher lived from 1898 to 1972. There are numerous examples of Escher’s work, most of which is highly mathematical, available in books, on T-shirts, the “fifteen puzzle”, coffee mugs, jigsaw puzzles, to name just a few.

One of Escher’s major preoccupations was with producing space-filling designs or tessellations of the plane. He derived much of his inspiration for this in his first visit to the Alhambra in Spain in 1922, where he studied the truly stunning Moorish mosaics on the walls and floors. However, unlike the Moors, who were forbidden to use “graven images” and who therefore only made tiling patterns with geometric shapes, Escher attempted to completely cover the plane (i.e. create tessellations) with shapes that represented objects, such as animals or birds.

I was lucky enough to visit the Alhambra in 1996. Not only was I totally overwhelmed by the tiles and patterns, but it was easy to see how Escher had been influenced by the designs and used these as scaffolds for his plane tessellations.

Ernst (1994) discusses Escher’s early (and largely unsuccessful) attempts at producing space-filling designs, based on recognisable objects. He also alludes to some of the mathematical ideas underlying Escher’s work and mentions links with crystallography.

Schattschneider (1990), in her magnificent book *Visions of Symmetry: Notebooks, Periodic Drawings and Related Work of M. C. Escher*, describes, in great detail, Escher’s “route to regular divisions” and the role that mathematics played. Escher’s early unsuccessful attempts at regular divisions of the plane, using recognisable objects, were produced during the five years after his first visit to the Alhambra in 1922. In 1936, Escher revisited the Alhambra in Granada and La Mezquita in Córdoba. He used his collection of detailed sketches of the geometric designs he had seen to provide the scaffold for his interlocking designs.

The geometric tilings copied in the Alhambra yielded many new insights to Escher, who found himself not just tinkering with the polygon shapes to derive new motifs, but also trying to discover the distinct ways in which individual figures could interlock with adjacent copies of themselves. (Schattschneider, 1990, pp. 19–20)

While this was the beginning, Escher was still struggling to produce the types of designs he desired. He described his explorations as follows:

I saw a high wall and as I had a premonition of an enigma, something that might be hidden behind the wall, I climbed over with some difficulty. However, on the other side I landed in a wilderness and had to cut my way through with great effort until — by a circuitous route — I came to the open gate, the open gate of mathematics. From there, well-trodden paths lead in every direction, and since then I have often spent time there. Sometimes I think I have covered the whole area. I think I have trodden all the paths and admired all the views, and then I suddenly discover a new path and experience fresh delights. (Escher, cited in Schattschneider, 1990, p. 21)
The “open gate of mathematics” came to Escher via his half brother B. G. (Beer) Escher, a professor of geology, who, on being shown Escher’s work, recognised that he was applying some form of two-dimensional crystallography and provided him with a number of papers published in Zeitschrift für Kristallographie between 1911 and 1933. Of these, the one that had a profound influence on the work of Escher was Pólya’s (1924) paper that classified the 17 plane symmetry groups (also known as the wallpaper groups). While this result — that there are just 17 different essentially different ways to repeat a design in the plane — was known, Pólya provided an illustration for each of the 17 possible tilings, including four of his own design (Schattschneider, 1987, 1990). Escher copied Pólya’s article in full and studied the illustrations to understand their geometric structure, and how “these tilings could be colored with a minimum number of colors in a way that was compatible with the symmetries of the tiling” (Schattschneider, 1987, p. 295). Pólya and Escher corresponded, but Pólya left the correspondence behind when he departed from Zurich in 1940. Schattschneider found Escher’s notebook with the single word “Pólya” written on the cover in a museum in The Hague in 1976. She sent her photograph of it to Pólya, who then told her of his correspondence with Escher (Schattschneider, 1987).

Given Escher’s huge popularity, it is not surprising that almost all students are fascinated by his work. They may also have heard about Pólya, often referred to as “the father of modern problem solving”. At the same time, much of the mathematics that is so superbly illustrated by Escher’s work occurs frequently in school mathematics curricula. For example, in Victoria, the Victorian Essential Learning Standards — VELS (Victorian Curriculum and Assessment Authority, 2005) refers to various aspects of symmetry, transformations and tessellations at every level from Level 2 to Level 6. As Motterhead (1977) so beautifully illustrates, the learning of geometry can be tremendously enriched by exposing students to Escher’s work, and the underlying mathematical concepts.

Conclusion

In this paper, I am not trying to advocate adopting a history of mathematics approach to the teaching of mathematics, but rather to encourage us all to attempt to contextualise the mathematics that we teach, to show the links to its applications and the connections between various aspects, and to reveal the people, who create the mathematics, to our students. For most students, it is a surprise to hear that mathematics is actually created by people — some of whom are alive, or have only recently died.

While none of the examples used here are new they, nevertheless, illustrate some ways in which contemporary mathematics can be, and is, used in real life. We talk a lot about the importance of making mathematics relevant for students, but often this is understood to mean that the mathematics should be used by students in everyday life — a hard ask that often leads to a trivialisation of the mathematics we teach. Of course, assembling such examples, and adapting them to an appropriate level to suit students in one’s class, is not easy. However, we do not need to develop examples for every topic. Instead, I believe that we should take the opportunity, every now and then, to look at some genuine applications in some depth. Such examples also allow us to make connections between different areas of mathematics (for example, prime numbers, factorisation and modular arithmetic, in the case of public-key cryptography). They also show the essential nature of mathematics and just how widespread its applications are (for example, the “open gate of mathematics” that enabled Escher to develop his wonderful designs for regular divisions of the plane).
Most of all, this paper attempts to persuade teachers of mathematics to convey to their students the joy of mathematical discovery — something that is often forgotten at a time when there is a real crisis in the number of students wanting to pursue higher studies in mathematics and, when, it is becoming increasingly difficult to find teachers for those students who do wish to pursue such studies.

References


