HISTORY OF MODERN APPLIED MATHEMATICS IN MATHEMATICS EDUCATION

UFFE THOMAS JANKVIST [1]

When conversations turn to using history of mathematics in classrooms, the referent is typically the old, often antique, history of the discipline (*e g*, Calinger, 1996; Fauvel & van Maanen, 2000; Jahnke *et al*, 1996; Katz, 2000). [2] This tendency might be expected, given that old mathematics is often more closely related to school mathematics However, there seem to be some clear advantages of including histories of more modern applied mathematics or histories of modern applications of mathematics [3]

One (justified) objection to integrating elements of the history of modern applied mathematics is that it is often complex and difficult. While this may be so in most instances, it is worthwhile to search for cases where it isn't so I consider three here. The two first are examples of modern applied mathematics, more precisely the early history of error correcting codes (Shannon, Hamming, and Golay) and the early history of data compression (Huffman). The third is an example of a modern application of (old) mathematics, the history of public-key cryptography. I use these cases to examine possible effects of the history of modern applied mathematics on teaching and learning, as well as what differences may arise in using newer histories of mathematics

I distinguish between the use of history in mathematics education as (1) a tool, in the sense of assisting the actual learning of mathematics (mathematical concepts, theories, and so forth), and as (2) a goal in itself, for example, by bringing about meta-aspects concerning the history of mathematics in mathematics education (*e g*. Jankvist, 2007; Jankvist, in press).

By *meta-aspects*, I am thinking of posing and responding to questions such as the following, drawn from Niss (2001, p 10):

- How does mathematics evolve in time and space?
- What forces and mechanisms cause the evolution of mathematics?
- How does the evolution of mathematics interact with society and culture?
- Can mathematics become obsolete?

Whereas *history as a goal* is concerned with teaching and learning something about the meta-aspects of the evolution and development of mathematics, *history as a tool* is concerned with the teaching and learning of the inner issues, or *in-issues*, of mathematics. When using history as a tool to improve learning or instruction, we may distinguish at least two different uses: history as a motivational or affective tool, and history as a cognitive tool Together with history as a goal these two uses of history as a tool are used to structure discussion of the educational benefits of choosing a history of modern applied mathematics.

History as a goal 'in itself' does not refer to teaching history of mathematics *per se*, but using history to surface meta-aspects of the discipline Of course, in specific teaching situations, using history as a goal may have the positive side effect of offering students insight into mathematical in-issues of a specific history But the important detail is whether one's intention is to use history as a goal or a tool With this framework in mind, I ask:

- How might a history of modern applied mathematics assist in the teaching and learning of in-issues of mathematics, both concerning the motivative/affective side as well as the cognitive side of using history as a tool?
- What meta-issues in terms of history as a goal might a history of modern applied mathematics make accessible to students?

Discussions of these issues are supported by empirical data from two of the cases. In 2007, cases 1 and 3 were implemented in a Danish upper secondary class. Danish upper secondary lasts three years. At the end of second year a class of 26 students took part in a module on case 1. A few months into their third year, the same class of 23 students took part in a module on case 3. Each module was taught by the regular teacher and spanned about fifteen 90-minute lessons. Specifically designed teaching materials were used (Jankvist, 2008c; Jankvist, 2008d). Classes were videotaped, questionnaires were given to students before and after each module, and 10–12 students and the teacher were interviewed before, between, and after the modules. At the end of each module students wrote an essay on aspects of the history. [4]

The historical dimension: a study of three cases

With the birth of the computer era, mathematicians found new ways to apply elements of discrete mathematics - both in creating new mathematical disciplines and in solving various 'computational' problems Three cases follow.

Case 1: The early history of error correcting codes

In 1948 Claude Shannon, at Bell Labs, published *Mathematical Theory for Communication* (Shannon, 1948) - the genesis of information theory. Shannon considered both channel coding (*i.e.*, error correcting codes to adjust for noise-induced errors during transmission - see fig. 1) and source coding (*i.e.*, compression of data for transmission).

Shannon proved that 'good' error correcting codes exist, but his proof gave no hints on how to construct them. He did provide one example of a good (efficient) code, namely the *Hamming (7, 4)-code*, through which he nodded to Richard Hamming.

Hamming, also at Bell Labs, used relay-based computers with error-detecting codes. Unfortunately, whenever they detected an error they halted and had to be reset. After having his work dumped two weekends in a row, Hamming was prompted to create codes that enabled computers to correct occurring errors (to a limited extent) and proceed with calculations. He used the generalized concept of *metric* to define what is now known as the *Hamming distance*. He also drew on vector space theory and linear algebra, thinking of possible binary n-tuples as coordinates of corners of an n-dimensional cube and his codes as subsets of these corners. Figure 2 illustrates that the Hamming distance between two codewords 111 and 101, written as $d(111, 101)$, is 1 since these two corners of the cube are one apart (or the codewords differ in exactly one place).

In order to determine the error correcting capabilities of a given code, Hamming introduced spheres. A sphere is centered in a codeword and the n-tuples inside or on the boundary of this sphere may be corrected into the codeword in the center (*i.e.*, they are at most the 'distance' of the radius away from the codeword). A code for which all the possible n-tuples are included in spheres around the codewords is called a *perfect code*.

Hamming-codes are perfect codes. To illustrate, consider the calculations for the binary (7, 4)-code. The space consists of $2^7 = 128$ different 7-tuples; $16 = 4^2$ of these being codewords chosen in such a way that any two codewords are always at a distance of at least 3. For every codeword there are seven other tuples that only differ in one place that may be packed into a sphere of radius 1 around the codeword. Calculating $(1 + 7) \cdot 16 = 128$ shows us that no tuples in the space are left outside a sphere; thus the code is perfect.

Due to patent delays Hamming's (1950) article on error correction wasn't published until two years after Shannon's. By then another mathematician, Marcel Golay, had generalized the (7, 4)-code presented in Shannon's article to all other Hamming codes (Golay, 1949) - prompting a dispute over the actual creator of the family of codes (Thompson, 1983, pp. 56–59). Golay invented four additional codes, of which two are perfect. One of these, a tertiary (23, 12)-code called G_{23}, is especially interesting. Coding theoreticians in 1973 proved it the only (non-trivial) perfect code that may correct three or more errors - practically halting further quests for perfect codes.

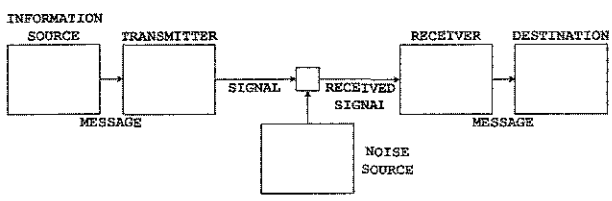

Figure 1: Shannon's illustration of a system of communication (Shannon, 1948, p. 5) [5]

Case 2: The early history of data compression

In 1951 Robert M. Fano gave the students in his information theory course a choice between a final exam and a term paper. The term paper assignment seemed simple: find the most efficient method of representing numbers, letters, or other symbols using a binary code.

Among the students opting for the paper was 25-year old David A. Huffman. Through months of effort, he arrived at several methods, but none could be proven the most efficient. Just before giving up, the solution came to him (Stix, 1991, p. 54).

His idea was to assign the shortest binary codes to the symbols occurring most often, drawing on the concept of a coding tree. To illustrate, consider the string ALIBABA. The frequency of A, B, I, and L in this string are $^3/_7$; $^2/_7$; $^1/_7$; $^1/_7$. A coding tree consists of branches and leafs, each leaf representing a symbol and an associated frequency or probability. In Huffman's algorithm the least probable symbol is first assigned to a leaf. We have two, I and L, so our tree consists of two leaves each with the associated probability of $^1/_7$, two branches, and a root with a summed up probability of $^1/_7 + {}^1/_7 = {}^2/_7$ (see fig. 3). The next less probable symbol, B, is then added, and probabilities are assigned and summed up. Last, A is added, resulting in a probability at the root of $^7/_7 = 1$, terminating the algorithm. The binary codewords are now assigned the letters by means of traversing the tree: 0 if traversing a branch to the left and 1 traversing a branch to the right. In this way we get A $\mapsto$ 0, B $\mapsto$ 10, I $\mapsto$ 110, and L $\mapsto$ 111.

I won't present the proof that Huffman's (1952) method works. (It can be developed by introducing a few elementary concepts of data compression codes - see *e.g.* Sayood, 2000; Solomon, 1998.) Its success rested on the fact that the least probable symbols are assigned to the outermost leaves,

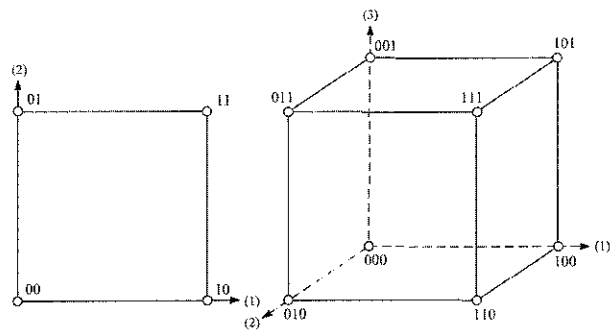

Figure 2: Binary tuples of length 2 pictured as points in the plane, and binary tuples of length 3 pictured as points in space (Jankvist, 2008c, p. 39)

thereafter moving along the branches to the root Shannon and Fano had attacked the problem in the opposite direction, giving in a less optimal solution.

Case 3: The history of public-key cryptography and RSA

The third type of mathematical coding, cryptography, concerns keeping information secret. A thousands-year-old problem in cryptography is that of distributing the private encryption and decryption key between two parties. In 1975, cryptographers at Stanford University provided two solutions: a safe way to generate a common integer (*i.e.* the key, between two parties), and public-key cryptography, a new system.

Whitfield Diffie had the revolutionary idea behind this scheme. He wondered if there might be a one-way function – that is, a function f which, for every x in its domain, $f(x)$ is easily calculated, but for every $y = f(x)$ in its range, $f^{-1}(y) = x$ is impossible to calculate for all practical purposes. The idea behind 'for all practical purposes' is that it may take seconds to calculate the function in one direction but eons to calculate the other way. For example, a person – Bob – by means of a one-way function generates a public encryption key; one to which only he knows the decryption key (*i.e.* the inverse function). Another person – Alice – who wants to send a secret message to Bob uses his key, posted somewhere public, to encrypt the message. Bob is the only one able to decrypt the message. Due to the nature of the one-way function, a cryptanalyst – Eve – eavesdropping on the line would stand little chance of breaking the code even though she knows both the encrypted message and the public key. The situation is illustrated in figure 4.

Diffie and Hellman spent almost a year looking for a suitable one-way function before giving up and publishing the idea in 1976. Ronald Rivest and Adi Shamir at MIT found this paper and took it on, developing ideas and passing them on to Leonard Adleman for testing. After Adleman had shot down 42 efforts, Rivest came up with a winner (Bass, 1995) by drawing on number theory – specifically the prime factorization of large numbers.

Generating a very large number n of, say, 200 digits by multiplying two also-large primes p and q is straightforward. However, the other way is 'for all practical purposes' impossible. Rivest devised a method for generating both public and private keys relying on this one-way function. The public encryption key consisted of two numbers, n and e, the latter of which was determined so that $\gcd(e, (p-1)(q-1)) = 1$. The encryption procedure E on the message M revealing the cipher text C was defined as $C \equiv M^e \pmod{n}$. The private decryption key, besides also consisting of n, consisted of a number d that was an inverse of e modulo $(p-1)(q-1)$, which is to say that $ed \equiv 1 \pmod{(p-1)(q-1)}$. The decrypting procedure D was defined as $C^d \equiv M \pmod{n}$.

Of course it had to be proven that the decryption procedure led to the original message M. Rivist, Shamir and Adleman (1978) did this with established – even antique – number theory, using Euler's theorem (1735-36), Fermat's little theorem (1640), and the Chinese remainder theorem (around 4th century). They patented the procedures and, in 1982, started a company offering RSA-solutions. It was sold in 1996 for $200,000,000.

As an interesting twist, it was made public in 1997 that the British Government Communication Headquarters (GCHQ) already knew of the system in 1969 (see Singh, 1999). During the 1960s the British military had considered equipping soldiers with radios to be in constant contact with their superiors. However, the distribution of keys imposed a problem. GCHQ cryptographer James Ellis was asked to look into the problem. By 1969 he arrived at the same idea that Diffie reached six years later. And just as Diffie and Hellman later would not be able to identify a suitable one-way function, neither could Ellis. He and the rest of GCHQ knew there was a solution in theory, but it was four years before a young number theoretician, Clifford Cocks, offered one within a half-hour of learning of the 'crazy' idea. Four years later it proved to be identical to that of Rivest, Shamir and Adleman.

As a secret organization, GCHQ was not interested in publicizing (and hence patenting) discoveries. Consequently, Ellis and Cocks silently watched as others were credited, honored and lucratively rewarded. In the early 1980s Diffie learned about Ellis's work and, in 1982, visited to set the record straight. All he managed from Ellis was a comment about the academics having done much more with it than GCHQ ever had (Singh, 1999).

The educational dimension: a discussion based on the three cases

I now consider the use of history of modern applied mathematics in terms of history as a tool, looking first at the motivational/affective side and then at the cognitive side. I then address the use of history as a goal in terms of the meta-aspects histories of modern applied mathematics may illustrate [6].

The motivational/affective side of history as a tool

At the completion of the module on case 3, students were asked which of the two histories they found to be the most

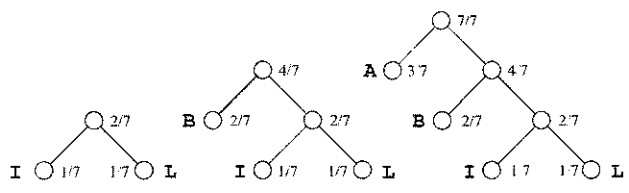

Figure 3: Building a binary Huffman tree for the string ALIBABA

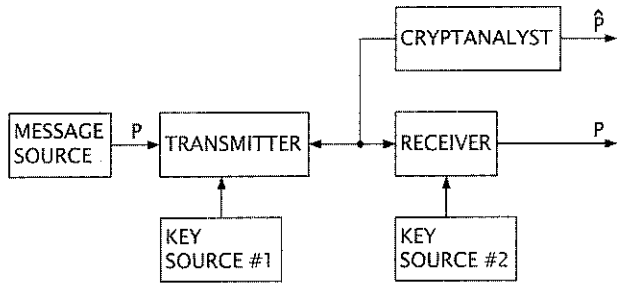

Figure 4: Diffie's and Hellman's illustration of public-key cryptography (Diffie & Hellman, 1976, p 647)

interesting and why. Most of their answers dealt with the motivational and/or affective side of using history as a tool.

The fact that the history is a newer and fairly recent history of mathematics seems to make it easier for the students to relate. To illustrate:

> Student: The newest, because it was most 'high tech' or whatever you may call it. It's alright that this guy Euclid did something too ... but these three guys, or six, or how many they were, that I thought to be much more exciting because they are still alive. It's almost 'just around the corner' that they invented it and yet it is so widely used now [..]
>
> Interviewer: Is it easier to relate to?
>
> Student: I think so. It's kind of difficult imagining a guy doing something before Christ was born ...

So, besides being more recent, it also matters that the characters are either still alive or have lived during the students' or their parents' lives.

Concerning the history of modern applications of mathematics some students may find it more interesting to work with such a history, and possibly even more so if they recognize elements from everyday life:

> Student: I think the new one, because you touch much more upon this applied mathematics and learn that mathematics is being used for something ... because many in the old history, they were hobby mathematicians and such. They just did mathematics to do mathematics, to show that they could. I don't find that as exciting, just doing something for the sake of doing it. So I think the new one was the most exciting one.
>
> Interviewer: Because it was applied?
>
> Student: Yes, because you were being told stuff about how it was put to use.

The three cases are examples of how mathematics may be put to use. Error correcting codes are used whenever data are transmitted or stored digitally. Most often more advanced codes than Hamming's are used, although Hamming codes are still implemented in some computer hardware. Data compression is used at least as often, since data are usually compressed before transmission or storage. In spite of their age, Huffman codes are still among the most used data compression codes. RSA is widely used on the Internet – in email, online banking, and so on. However, for much of the mathematics encountered in school, where it might be applied may not be so obvious.

When I asked in the first interviews where the mathematics learned in class was used, besides basic calculations, a common answer was: "In school!" This, of course, touches upon the discussion of the mathematics applied in our society and everyday lives being hidden. That is, it is embedded in technology such as computer chips, it infuses laws and other decision making processes, and so on (see Jankvist & Toldbod, 2007; Niss, 1994).

For these reasons some students find the newer history to be more relevant, as one student related:

> I think because the development of the Internet is somewhat more relevant to us and it's just a little more fun when it takes place in more recent time. ... Well, with Euclid and Fermat it wasn't like 'Yeah!'. But I thought that these newer researchers and their ways of doing things, the order in which events took place, and the fact that several people invented it at the same time, that was exciting.

Seeing newer history as more 'exciting' was often mentioned. One student made the point this way:

> The closer it comes to our present time, the easier it becomes to draw parallels, right, then it becomes more exciting. And then if it is something you do every day and then suddenly are being told, well okay that's where it comes from. I think it is very exciting knowing how things are.

When discussing mathematics in everyday life, the same student remarked:

> I didn't realize at all that the messages we are sending over the Internet and such, that it was mere mathematics.

Of course, interview data like these must be treated cautiously. One never knows if comments are efforts to reflect what the interviewer wants to hear. However, questionnaires, essays, and video records indicate that the interview data provide a good 'marker' of student beliefs.

The cognitive side of history as a tool

Hamming's way of developing his codes may serve as an introduction to the concept of distance in general. In the implementation of case 1, most students did not realize there could be more to it than euclidian distance. The fact that there is a 'spatial' meaning in the binary case also surprised many. Hamming's use of elements of linear algebra and the concept of linearity may also be useful in introducing matters related to these topics.

Case 3 offers the possibility of introducing number theoretic concepts to students and showing how they play together in a real application. For instance, properties of prime numbers, the euclidian algorithm, calculating modulus, congruence, and linear congruence are all needed to get RSA to function. In the implementation of case 3, the students knew nothing about number theory prior to the module, so cryptography and RSA served as a way into this discipline.

In case 2, Huffman's method may serve to introduce the notion of algorithm. Given that the mathematics involved is quite different from common curriculum mathematics, the modern history might not be the most obvious choice on

the cognitive side. Some exceptions occur, of course - as, for instance, in the case of the Danish upper secondary mathematics program where the teachers fill in one third of the curriculum, in consideration of general goals such as applications, modeling, and historical aspects

Meta-aspects in terms of history as a goal

I return now to the four questions mentioned earlier (drawn from Niss).

On the matter of *how mathematics evolves in time and space,* a newer history may be as effective as an old one in locating the evolution of mathematics. A history of a modern application of old mathematics may even draw parallels between time and space. Case 3 is a good example. In its implementation, students worked with both old and new in being asked to discuss personal motivations of an older mathematician and to relate these to the general discussion of inner and outer driving forces in number theory. They did the same for more contemporary mathematicians involved in cryptography and then contrasted the accounts. The following quote encompasses the more fragmented answers of some of the other groups:

> [I]t is quite clear that the period under in which mathematicians live has great influence on mathematical research being conducted. In older times mathematicians did mathematics out of a desire to do so; often mathematics was a free-time activity or even a hobby. Mathematical research was driven from within, mathematicians sought to solve problems for the sake of mathematical research itself. In comparison, more contemporary mathematicians were influenced by external driving forces. As Hardy also points out, war is an outer driving force for mathematics. Often wars have raised new questions that afterwards have been solved by scientists in terms of developing new areas within their respective fields, including mathematics. Another clear outer driving force in this sense is money. This [war and money being outer driving forces] has, more or less, been the case for mathematicians like Diffie, Hellman, Ellis, Cocks, Rivest, Shamir, Adleman, *etc.* while the situation was different for Euclid, Fermat, Euler, Gauss, Riemann, and Hardy.

Concerning case 3, students also discussed the fact that the development of public-key cryptography and RSA took place more or less simultaneously in two different 'spaces'. Case 1 provides another good, but perhaps less obvious, example of such multiple discoveries/inventions. In this case, students considered Hamming's use of older established techniques. Such an approach of epistemic objects and techniques (*e.g.*, Epple, 2000) provide a good and useful way to illustrate mathematics in time and space since, for instance, what in one situation serves as a technique may earlier have been an object studied through other techniques.

As for the *forces and mechanisms behind the evolution of mathematics,* a newer history may offer some important access points. It may be that Hamming's annoyance with computers drove him to develop his codes. Huffman avoided an exam by solving a problem for a term paper assignment. Diffie and Hellman were driven by a fascination for the old problem of safely distributing cryptography keys.

Regarding *how the evolution of mathematics interacts with society and culture,* a newer history may offer students a more familiar route. Hamming became involved with computers during his work at the Los Alamos project in World War II. After the war he worked with computers at Bell Labs, by then a large research corporation greatly reliant on war-enhanced government funding. Shannon's development of information theory also had to do with computers entering the society, and Huffman's method for data compression may be seen as a direct consequence of Shannon's work. As for public-key cryptography and RSA, on one hand it was inspired by the early development of the Internet, but on the other hand it was aimed at more efficient warfare. Concerning this, as part of the implementation of case 3, students were to read most of Hardy's (1940) *A Mathematician's Apology* and used it in discussions of pure versus applied mathematics. For many groups, discussions veered toward mathematics and war - due to Hardy's writing. In fact, several students were intrigued and engaged by the extended use of mathematics in war. Opinions on Hardy included:

> [W]e believe Hardy's book to pose some interesting views even though we don't agree entirely with all of them. Applied mathematics isn't only misused in wars and politics, but also used to, for instance, build houses, *etc.*

> Mathematicians applying mathematics aren't 'the bad guys'. No, it is the governments who use the applied mathematics in wrong doings that are. Anyway, we believe mathematicians today to be somewhat indifferent since they probably don't believe that they are the ones responsible, but on the contrary the people who use the knowledge to do evil.

Ethics was not an explicit theme of the assignment. Nonetheless, some students clearly engaged with the issue.

Concerning *whether mathematics can become obsolete,* a history of modern applications of old mathematics may illustrate that we should be careful in ruling out any mathematics for later applications. It may also highlight the need for basic research. When asking to this in relation to case 3, one group replied:

> Hardy believes prime numbers and number theory to be one of the purest forms of mathematics. It has no practical applications. Therefore it cannot be used [applied] or misused. ... RSA may tell us that basic research in mathematics is quite important since RSA couldn't have been realized had it not been for the basic research from 200 years earlier. This doesn't fit well with Hardy's statements about number theory and primes.

Besides the above, looking to the history of modern (applied) mathematics rather than merely the history of old or antique mathematics may make it easier to show students that mathematics continues to develop.

Conclusion

Concerning the use of history as a goal in mathematics education, a history of modern applied mathematics may be as good a candidate as any In some respects it appears to be better than some.

As a tool, the history of modern applied mathematics has some strong motivational and/or affective qualities A newer history may also serve as a cognitive tool However, given the often-fixed boundaries of curricula, a newer history may not always be an obvious choice Of course, the suggestion is not to reject old history but, rather, to consider the history of modern applied mathematics when integrating the history of mathematics This should be done in accordance with one's original purposes - that is, taking into account the use of history as either a goal or a tool, and attending to the implications of a history of modern applied mathematics on these two different uses

Notes

[1] This paper is a modified version of one presented at the History and Pedagogy of Mathematics (HPM) 2008 in Mexico City

[2] See also proceedings from meetings such as HPM and European Summer University on the History and Epistemology In Mathematics Education; and special issues on history in journals such as *Educational Studies in Mathematics* and *For the Learning of Mathematics*

[3] Hereafter only referred to as *the history of modern applied mathematics*

[4] See Jankvist, 2008a, 2008b

[5] Encoding with error correcting codes takes place before the message reaches the transmitter Errors can occur as a result of the noise source Error decoding takes place after the message is received

[6] All the quotes from the research data are translated from Danish

References

Bass, T. A. (1995) 'Gene genie', *Wired Magazine* 3(08), accessible at http://www wired.com/wired/archive/3 08/molecular html

Calinger R (ed.), *Vita mathematica – historical research and integration with teaching* (MAA Notes, no 40), Washington, DC, The Mathematical Association of America, pp. 3-16.

Diffie, W. and M. E Hellman (1976) 'New directions in cryptography', *IEEE Transactions on Information Theory* **22**, 644-654

Epple, M (2000) 'Genisis, Ideen, Institutionen, mathmatischeWerksttten: Formen der Mathematikgeschichte - Ein metahistorischer Essay', *Mathematische Semesterberichte* **47**, 131-163.

Fauvel, J. and van Maanen, J. (eds.) (2000) *History in mathematics education – the ICMI study*, Dordrecht, NL, Kluwer

Golay, M. J. E. (1949) 'Notes on digital coding', *Proceedings of the IRE* 37, 657.

Hamming, R. W. (1950) 'Error detecting and error correcting codes', *Bell System Technical Journal* **29**, 147-160

Hardy, G H (1940) *A mathematician's apology*, Cambridge, UK, Cambridge University Press

Huffman, D. A. (1952) 'A method for the construction of minimum-redundancy codes', *Proceedings of the IRE* **40**, 1098-1101.

Jahnke, H N., Knoche, N and Otte, M. (eds.) (1996) 'History of mathematics and education: ideas and experiences, no 11' in *Studien zur Wissenschafts-, Sozialund Bildungsgeschichte der Mathematik* Göttingen, DE, Vandenhoeck & Ruprecht.

Jankvist, U. T and Toldbod, B (2007) 'The hidden mathematics of the Mars exploration Rover mission', *The Mathematical Intelligencer* **29**(1), 8-15.

Jankvist, U. T (2007) 'Empirical research in the field of using history in mathematics education: review of empirical studies in HPM2004 & ESU4', *Nomad* **12**(3), 83-105

Jankvist, U. T (2008a) 'Evaluating a teaching module on the early history of error correcting codes', in Kourkoulos, M and Tzanakis, C (eds.), *Proceedings 5th International Colloquium on the Didactics of Mathematics*, Rethymnon, GR, University of Crete

Jankvist, U. T. (2008b) 'A teaching module on the history of public-key cryptography and RSA', *BSHM Bulletin* **23**(3), 157-168

Jankvist, U. T (2008c) 'Kodningsteoriens tidlige historie - et undervisningsforløb til gymnasiet, No 459', in *Tekster fra IMFUFA*, Roskilde, DK, IMFUFA.

Jankvist, U. T (2008d) 'RSA og den heri anvendte matematiks historie - et undervisningsforløb til gymnasiet, No 460', in *Tekster fra IMFUFA* Roskilde, DK, IMFUFA.

Jankvist, U. T (in press) 'A categorization of the 'whys' and 'hows' of using history in mathematics education', *Educational Studies in Mathematics*.

Katz, V. (ed.) (2000) *Using history to teach mathematics: an international perspective* (MAA Notes no 51), Washington, DC. The Mathematical Association of America

Niss, M (1994) 'Mathematics in society', in Biehler, R , Scholz, R W , Sträßer, R. and Winkelmann, B. (eds.), *Didactics of mathematics as a scientific discipline* Dordrecht, NL, Kluwer pp 367-378.

Niss, M (2001) 'Indledning', in Niss, M (ed.) *Matematikken og Verden Fremads debatbøger – Videnskab til debat*, Copenhagen, DK Forfatterne og Forlaget A/S

Rivest, R L , Shamir, A and Adleman, L (1978) 'A method for obtaining digital signatures and public-key cryptosystems', *Communications of the ACM* **21**(2), 120-126.

Sayood, K. (2000) *Introduction to data compression* (2nd edn), San Francisco, CA, Morgan Kaufmann

Shannon, C. E (1948) 'A mathematical theory of communication I, II', in Slepian, D (ed.), *Key papers in the development of information theory* **27**, New York, NY. IEEE Press, pp. 379-423 and 623-656

Singh, S. (1999) *The code book: the secret history of codes and codebreaking* London, UK, Fourth Estate

Solomon, D. (1998) *Data compression. the complete reference*. New York, NY, Springer Verlag

Stix, G (1991) 'Profile: information theorist David A Huffman', *Scientific American* **265**(3), 54-55.

Thompson, T. M. (1983) *From error-correcting codes through sphere packings to simple groups* (Carus mathematical monographs, no 21), Washington, DC, The Mathematical Association of America

A 'Sticky' Problem

Given any six sticks of consecutive integral length (*e.g.*, 7, 8, 9, 10, 11, 12 cm), how many irregular tetrahedra are possible? (unknown origin, but of infinite variation; selected by Leo Rogers of the *Oxford Problem Café*)