HISTORY OF MODERN MATHEMATICS AND/OR MODERN APPLICATIONS OF MATHEMATICS IN MATHEMATICS EDUCATION

Uffe Thomas Jankvist
Department of Science, Roskilde University, P.O. Box 260, DK-4000 Roskilde
e-mail: utj@ruc.dk

ABSTRACT

The idea of this paper is to discuss the integration of history of modern mathematics and/or history of modern applications of mathematics in mathematics education as well as the possible teaching and learning benefits of introducing a newer history of mathematics over an old(er) one – something which seems to be done most often when integrating history. Three cases of the history of modern mathematics or modern applications of mathematics are presented and later discussed in terms of their possible contributions to the use of 'history as a goal' and 'history as a tool'. As a means for further illustration of this, empirical data from concrete implementations of two of the cases are also presented and discussed.

1 Introduction

When conversation falls on using history of mathematics in the teaching and learning of mathematics it is normally the old, often antique, history of mathematics which is suggested for integration (see e.g. Jahnke et al. (1996), Rowe (1996), Katz (2000), and Fauvel and van Maanen (2000)). This may perhaps not be that strange since the old mathematics often is closer related to the curriculum mathematics being taught at both primary and secondary levels of education, and to some degree also at tertiary levels. However, there seems to be some, more or less, obvious advantages of including the history of more modern mathematics or the history of modern applications of mathematics in mathematics education – these I shall return to. One (rightful) objection to integrating elements of the history of modern mathematics and modern applications of mathematics is, of course, that both modern mathematics and modern applications of mathematics often possess a high level in complexity and difficulty, both concerning the understanding and communication of it. But even though this may be so in the majority of cases, searching for and identifying the cases for which it isn't necessarily so is a worthwhile task to undertake. As a way to render this claim plausible I shall consider three concrete cases. The two first are examples of modern mathematics, more precisely (1) the early history of error correcting codes (work of Shannon, Hamming, and Golay) and (2) the early history of data compression (work of Huffman). The last is an example of a modern application of (old) mathematics, more precisely (3) the history of public key cryptography and especially RSA which relies on the Chinese remainder theorem, Fermat's little theorem, and Euler's theorem. The idea of this paper is to use these three cases as a basis for answering what effects modern mathematics and/or modern applications of mathematics may have on the teaching and learning of mathematics as well as what differences there may be between using these newer histories of mathematics as opposed to an old(er) history. In order to crystalize this broad aim into a couple of more specific – and to a higher extent answerable – research questions a small framework concerning why to use history in mathematics education, in general, will be provided.

1.1 A Proposed Framework

In the rest of this paper I shall 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, e.g. by bringing about meta-aspects of the history of mathematics in mathematics education (see e.g. Jankvist (2007b, pp. 91-92) or Jankvist (2007a, pp. 72-76)). By meta-aspects, or meta-issues, concerning the history of mathematics I am thinking of, for instance, posing and suggesting answers to questions like the following four (Niss, 2001, p. 10): (a) How does mathematics evolve in time and space? (b) What forces and mechanisms cause the evolution of mathematics? (c) How does the evolution of mathematics interact with society and culture? (d) And can mathematics become obsolete? So, where history as a goal is concerned with teaching and learning something about the *meta-issues* of the evolution and development of mathematics, history as

a tool is concerned with the teaching and learning about the inner issues, or *in-issues*, of mathematics.

1.2 Research Questions

With this framework in mind it is now relevant to ask the following questions:

- What meta-issues in terms of history as a goal may a history of modern mathematics or modern applications of mathematics make (easier) accessible to the students?
- How may a history of modern mathematics or modern applications of mathematics assist in the teaching and learning of in-issues of mathematics, both concerning the affective as well as the cognitive side of using history as a tool?

As already mentioned these questions will be discussed on the basis of three specific cases. However, in the discussion empirical data from concrete implementations of two of the cases will be included when relevant.

1.3 Background of Empirical Data

In the year of 2007 cases 1 and 3 were implemented in a Danish upper secondary class. Danish upper secondary takes three years in total At the end of second year a class of 26 students took part in a teaching module on the early history of error correcting codes (case 1). The same class, now counting 23 students, again took part in a teaching module, now on the history of public-key cryptography and RSA (case 3), a few months into their third year. Both modules stretched over approximately 15 double lessons, each double lesson lasting 90 minutes. Teaching materials designed specifically for the purpose were used (Jankvist (2008c) and Jankvist (2008d)). The class was taught by their usual mathematics teacher. The implementation was videotaped, questionnaires were given to the students before and after each module, and 10-12 students as well as the teacher were interviewed before, in between, and after the modules. At the end of each module the students were to do a rather large written essay-assignment concerning various aspects of the history they had been introduced to (for a more detailed description see Jankvist (2008a, in press) and Jankvist (2008b, in press)).

2 Three Cases from the History of Discrete Mathematics

With the birth of the computer era in the twentieth century mathematicians found new ways to apply elements of discrete mathematics both in creating new mathematical disciplines and in solving various 'computational' problems. This together with the fact that some elements of discrete mathematics stand a fair chance of being communicated to students in, at least, upper secondary school suggests that the history of discrete mathematics may be a place to look for relevant cases of the history of modern mathematics as well as modern applications of mathematics which may be used in mathematics education. In the following I shall outline the three historical cases mentioned above, three cases concerning mathematical coding of data.

2.1 Case 1: The Early History of Error Correcting Codes

In 1948 Claude Shannon, at Bell Labs, published his *Mathematical Theory for Communication* (Shannon, 1948) – the starting point of information theory. As part of this theory Shannon considered both channel coding, i.e. error correcting codes with the purpose of adjusting for any errors occurring during transmission as a result of noise (see figure 1), and source coding, i.e. data compression with the purpose of compressing the data to be transmitted. As part of his theory Shannon proved that 'good' error correcting codes exist. However, his proof wasn't a constructive proof, meaning that it gave no hints as how to construct such codes. But Shannon did provide one example of a good (efficient) code, namely the so-called Hamming $(7, 4)$-code which he gave with reference to Richard Hamming. (The code is called so due to the fact that every codeword, in the code, consists of seven binary symbols and out of these seven symbols the four are information symbols.) Hamming was another mathematician working at the Bell Labs. He was a user of the then quite large rely-based computers. These computers were using error-detecting codes, but every time they detected an error they would come to a halt and had to be reset. Hamming became quite annoyed with this after having his work dumped by the computer two weekends in a row. As a result hereof he created error correcting codes which enabled the computers to correct occurring errors (to a certain extent only, of course) and carry on

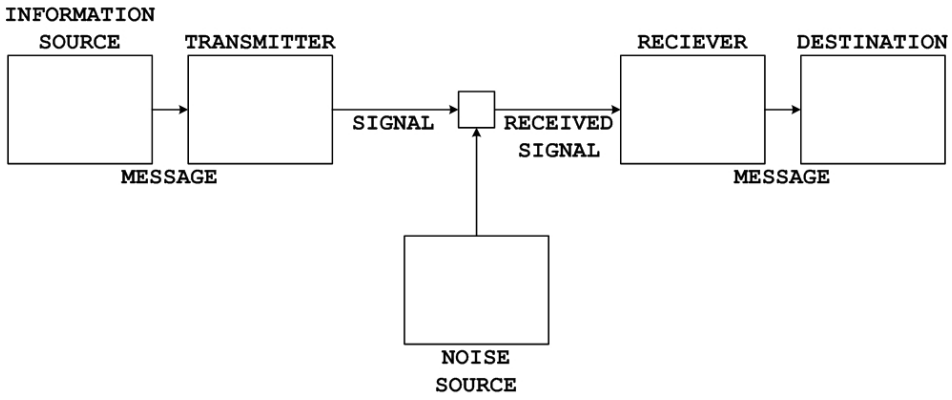

Figure 1: Shannon's illustration of a system of communication (Shannon, 1948, p. 5). Encoding with error correcting codes takes place before the message reaches the transmitter. Errors can occur as a result of the noise source. Error decoding takes place after the message is received.

with their calculations. Hamming used mathematics in his creation of the codes. For instance, he used the generalized concept of distance known as a metric to define what today is known as the Hamming distance. Also he used elements of vector space theory and linear algebra – he thought of possible binary n-tuples as the coordinates of corners of an n-dimensional cube and his codes as subsets of these corners. An idea of this may be obtained from figure 2. From this figure the Hamming distance between two codewords is also easily illustrated. For instance, the Hamming distance between the two codewords 111 and 101, written as $d(111, 101)$, is 1 since these two corners of the three dimensional 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 into his discrete metric spaces. A sphere is centered in a codeword and all the n-tuples inside or on the boundary of this sphere are the ones that may be corrected into the codeword in the center, i.e. they are at most the 'distance' of the radius of the sphere away from the codeword. Now, a code for which all the possible n-tuples are included in spheres around the codewords is called a perfect code. Hamming-codes are such perfect codes. To get an idea of this, let's do the calculations for the binary $(7, 4)$-code. The space consists of $7^2 = 128$ different 7-tuples, $16 = 4^2$ of these being codewords chosen in such a way that any two codewords always are a distance of at least 3 apart. For every codeword

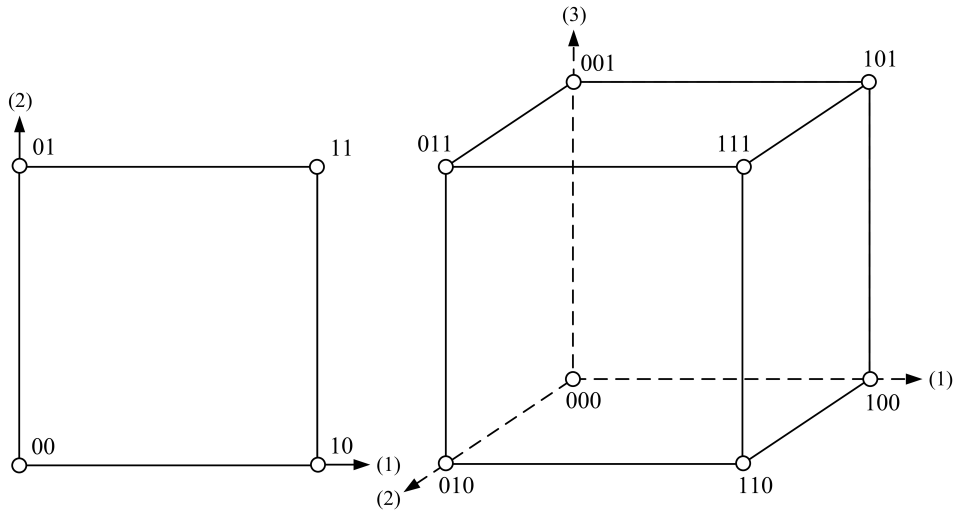

Figure 2: Binary tuples of length 2 pictured as points in the plane and binary tuples of length 3 pictured as points in space (Jankvist, 2008c, p. 39).

there are seven other tuples which 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 article on error correction (Hamming, 1950) wasn't published until two years after Shannon's article. At this point in time another mathematician, Marcel Golay, had already generalized the $(7, 4)$-code presented in Shannon's article to all other Hamming codes (Golay, 1949). This fact has led to an ongoing dispute about who actually can be called the creator of the family of Hamming codes (Thompson, 1983, pp. 56-59). Golay also invented a few additional codes, four to be precise, of which two are also perfect. Especially one of these, a tertiary $(23, 12)$-code called $\mathcal{G}_{23}$, is interesting since coding theoreticians in 1973 proved that this is the only (non-trivial) perfect code which may correct three or more errors, thus practically putting a stop to any further search for perfect codes.

2.2 Case 2: The Early History of Data Compression

As mentioned Shannon also considered the problem of effective data compression, but it was a graduate student at MIT who ended up providing the most efficient solution. In 1951 Professor Robert M. Fano gave the students taking his course on information theory a choice between a final exam and a term paper. The term paper assignment seemed simple: to find the most efficient method of representing numbers, letters, or other symbols using a binary code. Among the students was David A. Huffman, a bright 25-year old, who decided that he would rather do the paper than take the exam. What Huffman didn't know was that Fano, as well as Shannon, had been struggling with this problem for a few years – something which Fano didn't mention when giving out the assignment. Huffman worked on the assignment for months arriving at a number of methods, but none that could be proven to be the most efficient. However, just before giving up the assignment, and instead facing a final exam, the solution came to Huffman (Stix, 1991, p. 54).

Huffman's idea, like the ideas of many before him, was to assign the shortest binary codes to the symbols occurring most often. In devising his solution Huffman relied on the already available idea of a coding tree. Huffman's method is most easily explained by means of an example. Let's consider the string `ALIBABA`. The frequency of the letters `A`, `B`, `I`, and `L` according to 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 thus 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`, thus 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 figure 3). The next less probable symbol, `B`, is then added to the tree, probabilities are assigned and summed up. And last, `A` is added resulting in a probability at the root of $7/7 = 1$, thus 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` $\mapsto 111$.

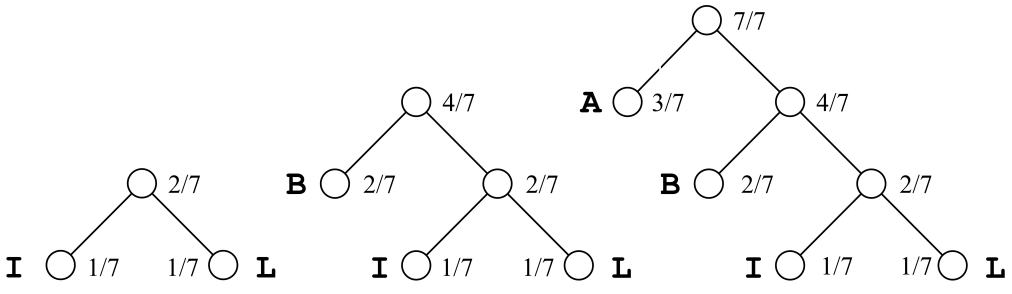

Figure 3: Building a binary Huffman tree for the string `ALIBABA`.

I shall not here carry out the proof that Huffman's method does, in fact, lead to the most efficient, or optimum, variabel length code. Such a proof may, however, be given fairly easy introducing only a few elementary concepts of data compression codes (see e.g. Sayood (2000) and Solomon (1998)). Worth mentioning, though, is that what made Huffman's method successful was the fact that he began by assigning the *least* probable symbols to the outermost leaves and then moving along the branches

to the root, meaning that he would arrive at an optimal solution every time. Shannon and Fano had attacked the problem in the opposite direction resulting in a less optimal solution. Today Huffman's solution to the assignment has probably become one of the most famous 'term papers' around, at least within the area of information theory, resulting in the publication (Huffman, 1952).

2.3 Case 3: The History of Public-Key Cryptography and RSA

One of the oldest problems in cryptography is that of distributing the private encryption and decryption key between two parties. After some two thousand years of having to deal with this problem it was finally solved in 1975 by a small group of cryptographers at Stanford University. Actually they solved the problem in two different ways, firstly by coming up with a safe way in which to generate a common integer, i.e. the key, between two parties, and secondly by proposing a totally new system of cryptography, public-key cryptograph, the one we shall deal with here. Whitfield Diffie was the one to get the revolutionary idea for this scheme. Early on in the 1970s Diffie had realized the potential of the so-called APRANet, which later was to develop into the Internet, as well as the need for keeping informations secret, e.g. in money transactions, in such a net. Diffie had then learned of Martin Hellman, another key-distribution 'fanatic' at Stanford and together with Ralph Merkle the three made up a team. But what was Diffie's idea? Well, Diffie thought, what now if we had such a thing as a one-way function: A function f for which it for every x in its domain is easy to calculate $f(x)$ but where it for every $y = f(x)$ in its range is for all practical purposes impossible to calculate $f^{-1}(y) = x$. Of course, the term 'for all practical purposes' isn't a well defined mathematical term, but the idea is that it may take seconds to calculate the function in one direction while it may take millions of years to calculate the other way. With this idea Diffie and Hellman was able to describe a new system of cryptography. The idea was that a person – Bob – by means of a one-way function generated a public encryption key, one to which only he knew the decryption key, i.e. the inverse function. Another person – Alice – who wanted to send a secret message to Bob could then use his public key, which would be posted somewhere public, to encrypt the message and send it to Bob who would then be the only one capable of decrypting this message. Due to the nature of the one-way function a cryptanalyst – Eve – eavesdropping on the line would stand no chance of breaking the code even though she knew 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 one-way function which would fit the description before finally giving up and publishing the idea of the system in 1976 (Diffie and Hellman, 1976).

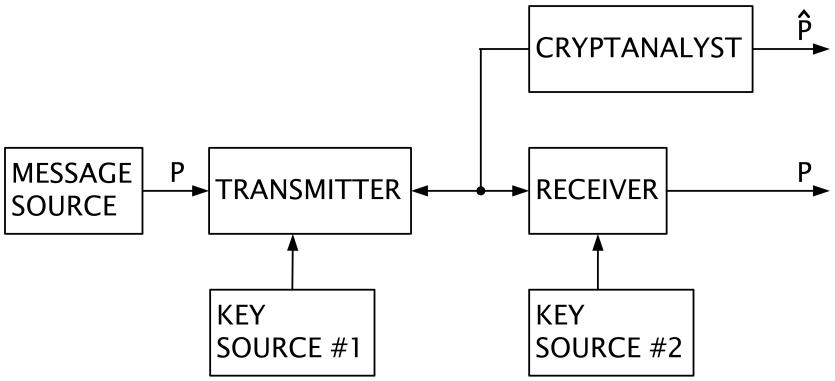

Figure 4: Diffie's and Hellman's illustration of public-key cryptography (Diffie and Hellman, 1976, p. 647). One public key (#1) is used to encrypt before transmission. Another private key (#2) is used to decrypt after reception.

Two computer scientists, Ronald Rivest and Adi Shamir, at MIT got hold of this paper and began a quest in search for the one-way function. Rivest and Shamir would come up with ideas and then pass them on to their friend and college, the mathematician Leonard Adleman, who would then put the ideas to the test. After Adleman had shot down 42 ideas Rivest came up with an idea which finally paid off (Bass, 1995). Rivest had turned his attention to number theory and especially the problem of prime factoring large numbers. Now, generating a very large number n, e.g. 200 digits, by means of multiplying two, also, large primes p and q is a straightforward operation. However,

going the other way is 'for all practical purposes' impossible. Using number theoretic results Rivest then 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 a number e which was determined in such a way that $\gcd(e,(p-1)(q-1))=1$, gcd being the greatest common divisor. The encryption procedure $\mathcal{E}$ 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 which was an inverse of e modulo $(p-1)(q-1)$, that is to say that $ed \equiv 1 \pmod{(p-1)(q-1)}$. The decrypting procedure $\mathcal{D}$ was defined as $C^d \equiv M \pmod{n}$. Of course it needed to be proved that the decryption procedure actually led to the original message M. Rivist, Shamir, and Adleman did this using well established – old and even antique – number theory (Rivest et al., 1978). More precisely they proved the result using Euler's theorem (∼1736), and the special case of this known as Fermat's little theorem (∼1636), as well as the Chinese remainder theorem (∼4th century). The encryption and decryption procedures due to Rivist, Shamir, and Adleman later became known as RSA (their initials). RSA was patented and in 1982 the three researchers started their own company offering RSA-solutions, a company which they sold in 1996 for the price of $200,000,000.

As an interesting twist to the history of public-key cryptography it was made public in 1997 that the British Government Communication Headquarters (GCHQ) already knew of the system back in 1969 (see Singh (1999, pp. 279-292)). During the 1960s the British military had been playing with the idea of equipping soldiers with radios in order for them to constantly be in contact with their superiors. However, it was soon realized that the distribution of keys eventually would impose a problem upon such a system. One of the top cryptographers of GCHQ, James Ellis, was asked to look into the problem. In 1969 Ellis had essentially arrived at the same idea as Diffie was to arrive at six years later. And just as Diffie and Hellman later wouldn't be able to identify a suitable one-way function so wasn't Ellis. For four years Ellis and the rest of GCHQ knew that their problem in theory had a solution but that they couldn't apply it without the crucial missing one-way function. In 1973 a young mathematician and number theoretician, Clifford Cocks, was employed by GCHQ. After six weeks in the department he learned of this 'crazy' idea of Ellis' and decided to look into it. Being so familiar with number theory Cocks was able to find a solution in no more than half an hour – a solution which four years later would prove to be identical to that of Rivest, Shamir, and Adleman. It took Cocks quite some time to realize the importance of the work he had done, but once he finally did he recalls thinking that his discovery would not have pleased the English number theoretician G.H. Hardy much (Singh, 1999, p. 286). GCHQ being a secret organization wasn't interested in making any of their discoveries public and therefor neither in patenting them. For this reason Ellis and Cocks had to silently watch from the sideline as the academics from Stanford and MIT got both the honor and money out of this new cryptographic invention. In the beginning of the 1980s Diffie learned, probably via the NSA, about Ellis' work. In 1982 Diffie went to Cheltenham to see Ellis and set the record straight, but all he got out of Ellis was a comment about the academics having done much more with it than GCHQ ever had (Singh, 1999, p. 290).

3 Discussion

In the following discussion I shall first consider the use of history of modern mathematics and/or modern applications of mathematics in terms of what meta-issues such histories may illustrate. Next, the use of history of modern mathematics and/or modern applications of mathematics in terms of history as a tool will be discussed, first regarding the motivational/affective side of using history as a tool and afterwards regarding the cognitive side.

3.1 Meta-Issues in terms of History as a Goal

It seems clear that a history of modern mathematics or one of modern applications of mathematics may bring out many of the same meta-aspects concerning the evolution and development of mathematics as any history of old mathematics may. I shall exemplify this by the four questions given in section 1.1.

(a) A newer history may just as well place the evolution of mathematics in both time and space. If it is a history of a modern application of old mathematics it may even draw parallels between the time and space in which the first development took place and the now modern application of this. Case 3 generates a good example in this respect. In the actual implementation of case 3 in Danish upper secondary the students were to work with two different histories of mathematics concerning

this case, namely the history of number theory (Euclid, Sun Zi, Fermat, Euler, Gauss, and Hardy) and the history of public-key cryptography and RSA (Diffie, Hellman, Rivest, Shamir, Adleman, Ellis, and Cocks). In the latter history the students also were to discuss the fact that the development of public-key cryptography and RSA took place more or less simultaneously in two different 'spaces' (GCHQ and Stanford/MIT). Case 1 provides another, maybe not as obvious but still, good example where the students in the actual implementation in their work with Hamming's development of coding theory were to consider his use of older already established techniques, especially Frchet's development of a metric (1906) and Grassman's study of n-dimensional spaces (1844) (see Jankvist (2008a)). (b) A newer history may describe, for the students perhaps even in a more familiar fashion, some of the forces and mechanisms which cause the evolution of mathematics. In the case of Hamming it was his annoyance with the way the computers were working. Huffman solved a problem given a term paper assignment by a daring professor and got out of an exam. Diffie was inspired by the beginning of the Internet and both him and Hellman were driven by a fascination of the 2000 year old problem of safely distributing cryptography keys. (c) A newer history may, also perhaps in a more familiar way, illustrate how the evolution interacts with society and culture. Hamming, for instance, had gotten involved with computers during his work at the Alomos project in world war 2. After the war he continued to work with computers at Bell Labs, a large research corporation relying to a great extent on the enhanced government funding as a result of the war. 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 this was on the one hand inspired by the early development of the Internet, i.e. computers (Stanford/MIT), but on the other hand as a means for conducting more efficient warfare (GCHQ). (d) Concerning whether or not mathematics can become obsolete, a history of modern applications of old mathematics, like that of RSA in case 3, may illustrate very well that we should be very careful in ruling out any mathematics for later applications.

Besides the above, looking at the history of modern mathematics as opposed to the history of old or antique mathematics may make it easier to show the students that mathematics is something which is still, even today, being developed.

3.2 The Motivational (and Affective) Side of History as a Tool

In the interviews after the completion of the module on case 3 the upper secondary students were asked which of the two histories of mathematics, the old or the new (and applied), they found to be the most interesting and why. Out of the 11 students asked, 1 seemed to think that the old history was slightly more interesting, 2 that they were of equal interest, and 8 that the new was definitely the most interesting. All these 8 answers had to do with the motivational and/or affective side of using history as a tool.[1]

Firstly, 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 this history.

> The newer history because it is something which is fairly close. And number theory is so long ago, it isn't as exciting as the newer, I'm not exactly sure why.
> *But what does it matter that it is closer?*
> That you can relate to it better.

> The newest, because it was most 'high tech' or whatever you may call it. Its 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. Its almost 'just around the corner' that they invented it and yet it is so widely used now. [...]
> *Is it easier to relate to?*
> I think so, it is kind of difficult imagining a guy doing something before Christ was born...

So, besides the history being of more recent date the fact that the historical characters are either still alive or have lived during the student's own, or their parents', lives also seems to have an effect in terms of motivation and affection. The students seemed to think it easier to relate to the characters as well as the historical circumstances under which they lived.

[1] All the quotes from the interviews presented in this section have been translated from Danish. Italics are used for the voice of the interviewer (me).

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 may recognize elements of it from their own everyday life.

> 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.
> *Because it was applied?*
> Yes, because you were being told stuff about how it was put to use.

The three cases from above are all examples of how mathematics may be put to use. Error correcting codes are used every time we either transmit or store data digitally (cell phones, CD-players, computers, just to mention a few). Most often more advanced codes than those of Hamming are used even though Hamming codes are still implemented in some computer hardware. Data compression is used just as often, if not more, since data usually is compressed before it is transmitted or stored (digital cameras, MP3-players, computers, etc., etc.). In spite of their old age Huffman codes still are some of the most widely used data compression codes today. RSA is widely used on the Internet, when we send emails, use our Internet banking systems, etc. However, for a lot of the mathematics which students see in school it may not be too easy to figure out where this might be applied, whether it be in society as a whole or in their own everyday lives. Of course, one may argue that the students often use the mathematics they learn in, for instance, the physics they are taught in school. That is true, but where then do they apply the physics they learn in school in their everyday lives? When I in the first interviews asked the students where they used the mathematics they learned in their mathematics class, besides from doing basic calculations, a not uncommon 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 to say that it is embedded in technology like, for instance, computer chips, it is inside laws and other decision making processes, etc., etc. (see e.g. Niss (1994) or Jankvist and Toldbod (2007)).

For the above reasons some students simply find the newer history to be more relevant:

> I think because the development of the Internet is somewhat more relevant to us and its 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 the newer history as being more 'exciting' is, as in the quotes above, something which several students keep mentioning:

> I think the new one. Because it was easier for me to see the present with Diffie's idea and that. They had discovered some theorems, but as described in the book, they kept on going even though they didn't get it exactly right the first 'one hundred' times. That I thought was exciting, that you could just keep on going. You don't think about it in your everyday.
> *So it had a connection to your everyday life or what do you mean?*
> Yes, I didn't realize at all that the messages we are sending over the Internet and such, that it was mere mathematics.

In an interview prior to this one the girl responsible for the last quote had exclaimed to the question of whether or not she thought that history of mathematics was something that might interest her, that it possibly would if it was an exciting story. In continuation of the quote above she was asked what characterized an exciting story for her:

> 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.

3.3 The Cognitive Side of History as a Tool

Besides being a tool in terms of motivating the students to learn the involved in-issues of mathematics the history of modern mathematics and modern applications of mathematics may also serve as a cognitive tool. Again I shall discuss this in terms of the three cases above.

In case 1, Hamming's way of developing his codes using discrete metric spaces may serve as an introduction for students to the concept of distance in general. In the implementation of case 1 in upper secondary, students mostly didn't realize that there could be more to the mathematical concept of distance than just the euclidian distance. Hamming's error correcting codes thus served as an example of exactly that. The fact that distance also had a 'spacial' meaning in the binary case surprised many students too. Also Hamming's use of elements of linear algebra, such as considering the codes as vectors in an n-dimensional space, as well as his use of the concept of linearity (Hamming and Golay codes are linear), may serve as a way of introducing matters concerning these mathematical topics to the students. Case 3 offers the possibility of introducing various number theoretic concepts to the students and almost imminently showing them how they play together in a real application of mathematics. For instance, properties about prime numbers, the euclidian algorithm, calculating modulus, congruence, linear congruence, as well as the Chinese remainder theorem, Fermat's little theorem, and Euler's theorem are all needed to get RSA to function. In the implementation of case 3 the upper secondary students knew nothing of number theory prior to the module, so in this case cryptography and RSA indeed served as a way into this mathematical discipline. In case 2 Huffman's method for finding the most efficient data compression may serve as a way for introducing the concept of an algorithm for the students, something which goes for case 3 as well of course. However, a problem with case 2 is that the mathematics involved may be quite far away from that of ordinary curriculum mathematics. Thus, the modern history may not always be the most obvious choice concerning the cognitive side of using history as a tool. Some exceptions do occur, of course, as, for instance, in the case of the Danish upper secondary school where the teachers themselves are to fill in 1/3 of the curriculum taking into consideration more general goals, such as treating applications of mathematics, mathematical modeling, historical aspects of the evolution and development of mathematics, to name a few.

4 Conclusion

From the discussion above it seems clear that a history of modern mathematics and possibly applications of this mathematics may be as good a candidate as any concerning the use of history as a goal in mathematics education, and in some respects it even appears to be a better one. Regarding the use of history as a tool the history of modern mathematics seems to have some very strong qualities concerning the motivational and/or affective side of this type of use. A newer history of, possibly applied, mathematics may also in some respects serve as a cognitive tool to the teaching and learning of mathematics. However, due to the often fixed boundaries of mathematics curriculum in many countries a newer history of mathematics may not always be the most obvious choice in this respect.

Of course, the arguments above for integrating a history of modern mathematics or modern applications of mathematics into mathematics education must not be seen as a reason for rejecting the use of the old and antique history of mathematics. Merely it is a suggestion of taking the history of modern mathematics and modern applications of mathematics into account when considering an integration of the history of mathematics. And when doing this, then doing it in accordance with the purposes one had of integrating history in the first place, i.e. taking into account the use of history as either a goal or a tool and the possible effects a history of modern mathematics or modern applications of mathematics may have concerning these two different uses of history.

REFERENCES

– Bass, T. A.: 1995, "Gene Genie". *Wired Magazine* **3**(08).

– Diffie, W. and M. E. Hellman: 1976, "New Directions in Cryptography". *IEEE Transactions on Information Theory*, pp. 29-40.

– Fauvel, J. and J. van Maanen (eds.): 2000, *History in Mathematics Education – The ICMI Study.* Dordrecht: Kluwer Academic Publishers.

– Golay, M. J. E.: 1949, "Notes on Digital Coding". *Proceedings of the IRE* **37**, p. 657.

– Hamming, R. W.: 1950, "Error Detecting and Error Correcting Codes". *Bell System Technical Journal* **29**, pp. 147-160.

– Huffman, D. A.: 1952, "A Method for the Construction of Minimum-Redundancy Codes". *Proceedings of the IRE* **40**, pp. 1098-1101.

– Jahnke, H. N., N. Knoche, and M. Otte (eds.): 1996, *History of Mathematics and Education: Ideas and Experiences*, No. 11 in Studien zur Wissenschafts-, Sozialund Bildungsgeschichte der Mathematik. Göttingen: Vandenhoeck & Ruprecht.

– Jankvist, U. T. and B. Toldbod: 2007, "The Hidden Mathematics of the Mars Exploration Rover Mission". *The Mathematical Intelligencer* **29**(1), pp. 8-15.

– Jankvist, U. T.: 2007a, "Den matematikhistoriske dimension i undervisning – generelt set". *MONA* **3**(3), pp. 70-90. English translation of title: The Dimension of History of Mathematics in Teaching and Learning – Generally Seen.

– Jankvist, U. T.: 2007b, "Empirical research in the field of using history in mathematics education: Review of empirical studies in HPM2004 & ESU4". *Nomad* **12**(3), pp. 83-105.

– Jankvist, U. T.: 2008a, "Evaluating a Teaching Module on the Early History of Error Correcting Codes". In: M. Kourkoulos and C. Tzanakis (eds.): *Proceedings 5th International Colloquium on the Didactics of Mathematics*. Rethymnon: The University of Crete.

– Jankvist, U. T.: 2008b, "A Teaching Module on the History of Public-Key Cryptography and RSA". *BSHM Bulletin* **23**(2).

– Jankvist, U. T.: 2008c, *Kodningsteoriens tidlige historie – et undervisningsforløb til gymnasiet*, No. 459 in Tekster fra IMFUFA. Roskilde: IMFUFA. English translation of title: The Early History of Error Correcting Codes – a Teaching Module for Upper Secondary School.

– Jankvist, U. T.: 2008d, *RSA og den heri anvendte matematiks historie – et undervisningsforløb til gymnasiet*, No. 460 in Tekster fra IMFUFA. Roskilde: IMFUFA. English translation of title: RSA and the History of the Applied Mathematics in the Algorithm – a Teaching Module for Upper Secondary School.

– Katz, V. (ed.): 2000, *Using History to Teach Mathematics – An International Perspective*, No. 51 in MAA Notes. Washington: The Mathematical Association of America.

– Niss, M.: 1994, "Mathematics in Society". In: R. Biehler, R. W. Scholz, R. Sträßer, and B. Winkelmann (eds.): *Didactics of Mathematics as a Scientific Discipline*. Dordrecht: Kluwer Academic Publishers, pp. 367-378.

– Niss, M.: 2001, Indledning. In: M. Niss (ed.): *Matematikken og Verden*, Fremads debatbøger – Videnskab til debat. København: Forfatterne og Forlaget A/S. English translation of title: Introduction to the book: Mathematics and the World.

– Rivest, R. L., A. Shamir, and L. Adleman: 1978, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". *Communications of the ACM*.

– Rowe, D. E.: 1996, "New Trends and Old Images in the History of Mathematics". In: R. Calinger (ed.): *Vita Mathematica – Historical Research and Integration with Teaching*, No. 40 in MAA Notes. Washington: The Mathematical Association of America, pp. 3-16.

– Sayood, K.: 2000, *Introduction to Data Compression*. San Francisco, California: Morgan Kaufmann Publishers, Second edition.

– Shannon, C. E.: 1948, "A Mathematical Theory of Communication I, II". In: D. Slepian (ed.): *Key Papers in The Development of Information Theory*, Vol. 27. New York: IEEE Press, pp. 379-423; 623-656. (Pages 5-18 and 19-29 in Key Papers in The Development of Information Theory.)

– Singh, S.: 1999, *The Code Book – The Secret History of Codes and Codebraking*. London: Forth Estate.

– Solomon, D.: 1998, *Data Compression – The Complete Reference*. New York: Springer Verlag.

– Stix, G.: 1991, "Profile: Information Theorist David A. Huffman". *Scientific American Special Issue on Communications, Computers, and Networks* **265**(3), pp. 54-55.

– Thompson, T. M.: 1983, *From Error-Correcting Codes through Sphere Packings to Simple Groups*, No. 21 in The Carus Mathematical Monographs. The Mathematical Association of America.