Martin–Luther–Universität
Halle–Wittenberg
Institut für Mathematik

John Neper's rods:
Calculations are boring and tiring!

Leon Battista Albert's Cipher Wheel

Wilma Di Palma

Report No. 04 (2009)

Reports on History of Mathematics

Editors:
Professors of the Institute for Mathematics, Martin-Luther-University Halle-Wittenberg.

Electronic version: see `http://www2.mathematik.uni-halle.de/institut/reports/`

John Neper's rods:
Calculations are boring and tiring!

Leon Battista Albert's Cipher Wheel

Wilma Di Palma

Report No. 04 (2009)

Wilma Di Palma
Responsible Museo della Matematica
del Comune di Roma "I Racconti die Numeria
Email: wdipalma@libero.it

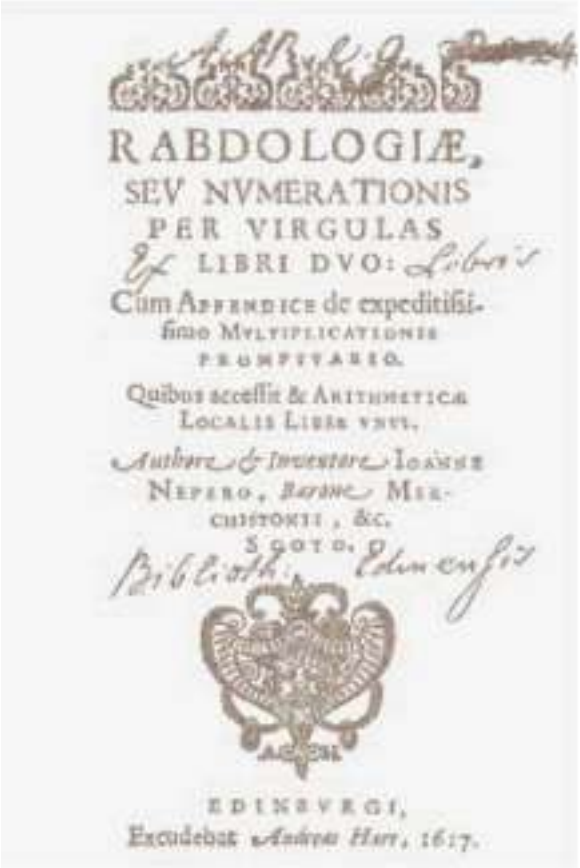
Neper's rods:
Calculations are boring and tiring!

John Napier, eighth Baron of Merchiston, was born at Merchiston Castle near Edinburgh in 1550. Those years were rather troubled for the Scottish Kingdom, because of religious and political fights between Catholics and Protestants, the former loyal to Mary Stuart, the latter supporting her son James VI of Scotland who hoped to succeed Elisabeth I to the English throne.

John Napier -or Neperus as he signed his latin works -was a passionate and uncompromising Protestant which turned out useful at the end of the civil war, when he was ten years old. He thought to gain over lasting fame because of his theological work (1594): *Plaine Discovery of the Whole Revelation of Saint John*, which occupies a prominent place in Scottish ecclesiastical history. However, his fame is really due to his contribution to Mathematics, a science he cultivated as a pleasant hobby.

Napier devoted most of his leisure to the study of Mathematics, in particular to devising methods of facilitating computations. Indeed, his name is associated with logarithms. The word "logarithm" was invented by Napier who put together the Greek words *logos* (ratio) and *arithmos* (number).

Life of both Mathematicians and Astronomers was made easier by the use of logarithms.



RABDOLOGIÆ,
SEV NVMERATIONIS
PER VIRGULAS
LIBRI DVO:
Cum Appendice de expeditissimo Multiplicationis promptuario.
Quibus accessit & Arithmetica Localis Liber vnus.
Authore & Inventore Ioanne Nepero, Barone Merchistonii, &c.
EDINBVRGI,
Excudebat Andreas Hart, 1617.

In the introduction to his book *Mirifici Logarithmorum Canonis Descriptio* (1614) Neper wrote: "Instead of having to face difficult and boring multiplications and divisions and having to extract roots, these operations can be taken out from the bulk of work and replaced by additions, subtractions and simple divisions by two and three".

The above mentioned book was followed by *Mirifici Logarithmorum Canonis Constructio* which appeared in 1619, two years after the Author's death.

However, even for such easy calculations some little help would have turned out useful. And the inventive Baron devised a simple and quick method to multiply any given positive integer (as big as you like) by the nine integers 1, 2, 3,..., 9.

And about this, here is what Neper himself wrote: "To calculate is a difficult and slow task and the boredom which comes from it is the main motivation for the dislike most people feel for Mathematics. I always tried - by all means at hand and all the power provided by my mind - to make easier and swifter such a process. Having such a goal, I devised the idea of logarithms ... at the same time, to the benefit of those who wanted to use positive integers only, I invented three more short methods for

simplifying calculations. The first one of these was called "Rabdologiae" and is based on the use of some rods on which the numbers are written..." (Ioanne Nepero, *Rabdologiae seu Numerationis per Virgulas Libri Duo,* Edinburgi, 1617).

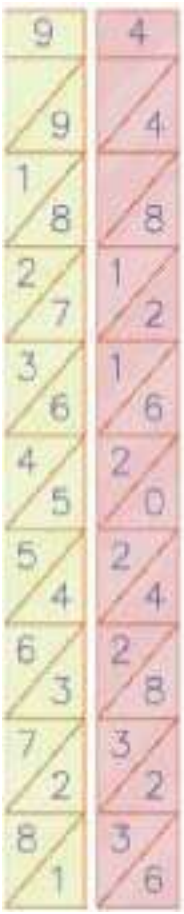
The rhabdomancy method uses a set of ten or more rods by which it is easy to find the result of otherwise very long computations. Such rods do not help in discovering springs as the name rhabdomancy might suggest! However, they help in finding something. Neper's original rods were made of ivory. This is the reason why they were nicknamed Neper's "bones", and such a name is still used in English speaking countries. This device was the forerunner of the slide rule.

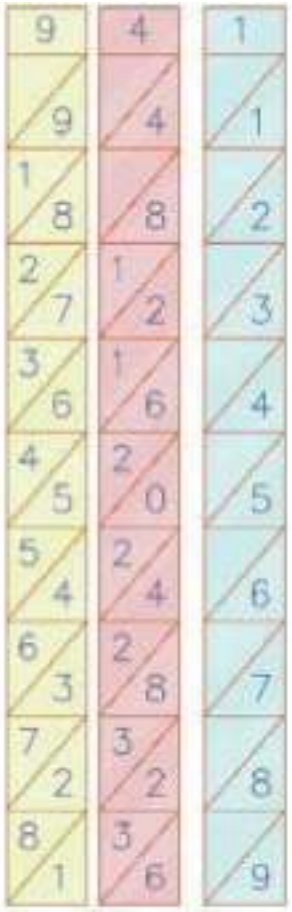
How to use Neper's rods.

First of all, each rod actually is a very elongated prism with square section. The rods are numbered, say one to nine, and usually there are copies of each one. On the rectangular faces the multiplication tables are printed of the integers 1 to 9. (The four faces of each rod may have engraved on them different multiplication tables.) Since just one rectangular face of each rod can be used at any time, to explain how multiplications are carried out we refer to such faces instead of to the whole rod (and you can easily construct your own "flat" Neper's rods).

On top a number is drawn which is the one whose multiplication table is considered on that face. For instance, the picture below represents the multiplication table of 4. The small squares of the face are each divided by one of the diagonals (the one from the top right corner to the bottom left corner), so that if the product consists of one digit only then it is in the right hand side triangle; when it consists of two digits, the first one is in the left hand side triangle (see picture). All this is not for aesthetic reasons, but is related to how the calculation instrument works as the example below will show.

Consider the following multiplication: 94 x 9.



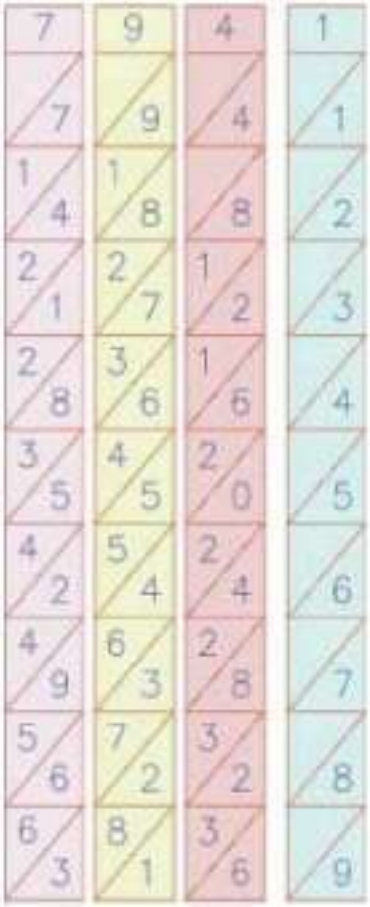


First of all, we put one next to the other the rods for 9 and 4 (this gives 94), then we put after them the rod for 1. Since we are multiplying by 9, we simply read the ninth line on these three rods (in the given order):

To obtain the result, we read these squares; the last digit will be 6, the last but one will be 3 + 1 (where the 3 comes from the second square and the 1 from the first one) and the first digit will be 8. Thus, 94 x 9 = 846.

Next, we want to multiply a three digit number, e.g. 794 x 7.

We take the rods for 7, 9, and 4 and set them as in the picture and, as before, we use the rod for 1 to find the relevant row. The seventh row (we are multiplying by 7) is



The result of this multiplication is as follows:

write the first number on the right: 8;

add 2 and 3 and get: 5;

add 6 and 9 and get 15, so write 5 and carry 1;

add 1 and 4 and get: 5.

Therefore, 794 x 7 = 5558.

You will recognise that this is what is usually done when multiplying:

28

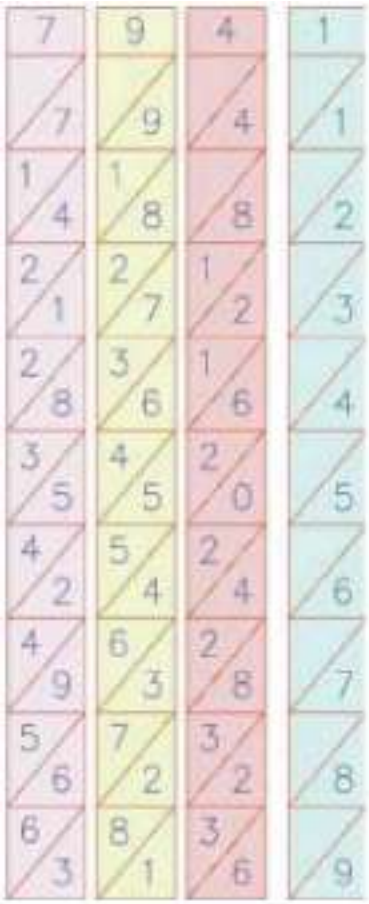
+ 63

+ 49

= 5558

The rule is the same for any number whenever the multiplier is a one digit number, that **is, 1, 2, 3, …. 9.**

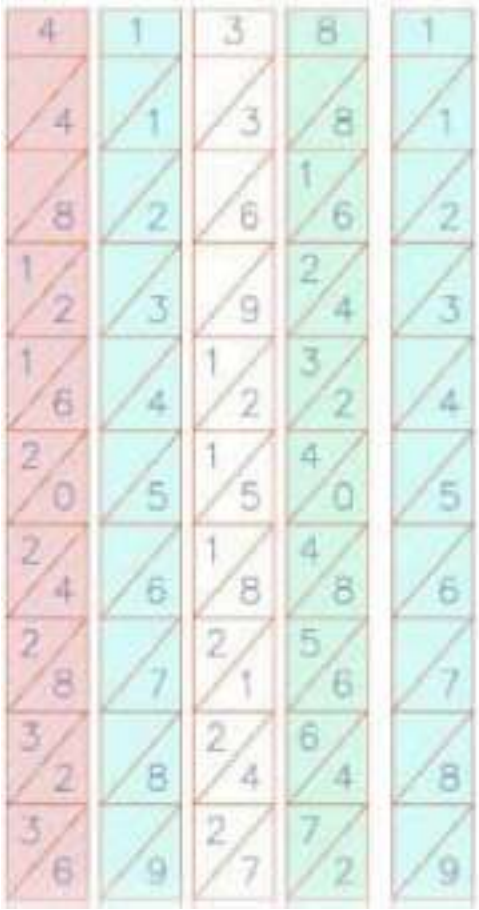
Next, we show how the rods work when we multiply by a two digit number.



By way of example, take 794 x 58. We use the relevant three rods to represent 794. Then we multiply this number by 5 which gives 794 x 5 = 3970; multiplying 794 by 8 yields 794 x 8 = 6352. Finally, we add these partial results:

```
  3970
+ 6352
  ------
= 46052
```

Our last example is 4138 x 567 which uses the four rods for 4, 1, 3, 8. The partial multiplication give



4138 x 5 = 20690

4138 x 6 = 24828

4138 x 7 = 28966

By adding these results we get

20690 +
24828 +
28966
————

= 2346246 Thus,

4138 x 567 = 2346246.

The rules are the same for all positive integers.

Indeed, nowadays computing machines exist which are more powerful and easier to use than the old Neper's "bones"; however, their use is still fascinating and "building" a multiplication is more satisfying and more fun than seeing the result on the display of a pocket calculator: a bit of reasoning does no harm!

References

-Boyer C. A History of Mathematics, John Wiley & Sons Inc, 1968
-Di Palma W. and Lamberti L.Le regole del regolo, Bollati Boringhieri, Torino 2000
-Kline M. Mathematical Thought from Ancient to Modern Time, 1972
-O'Connor J.J. and Robertson E.F. in URL
http://www-history.mcs.st-andrews.ac. uk/history/index. html
-Napier J. Rabdology,MIT Press 1999
-Napier J. English version Mirifici logarithmorum canonis descriptio in URL GW FW

Leon Battista Alberti's Cipher Wheel

Museo della Matematica del Comune di Roma "I RACCONTI DI NUMERIA"

Foreword

Rome's Mathematics Museum, "I Racconti di Numeria" ("Numeria's Tales"), opened to the public over ten years ago and allows visitors to "touch" mathematical culture and get rid of the idea that mathematical reasoning is too technical and difficult. We try to show the long way of Mathematics history by means of interactive exhibits which provide a straightforward grasping of some fundamental theorems and some most meaningful ideas. According to our experience, this is a good way to present Mathematics concepts which otherwise would remain abstract thoughts impossible to display in a museum. Obviously, elementary and high school pupils are our main public target and we devised some didactic kits the teachers can take to the class and perform again with their students what "learned" during the visit to the museum. Our last interactive didactic kit concerns the use of Leon Battista Alberti's cipher wheel.

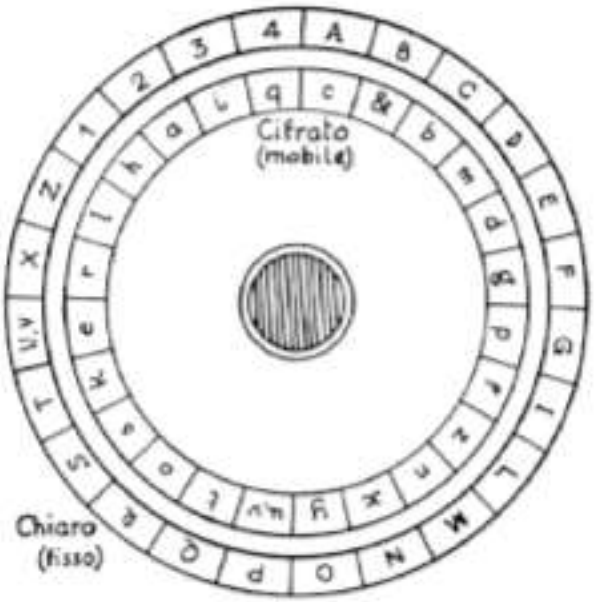
1. Leon Battista Alberti

Leon Battista Alberti (Genoa 1404 - Rome 1472) is a prototype of the Renaissance "universal man" whose versatility and accomplishments were vast and interwoven. He was a poet, scholar, architect and art theorist, and also worked in Mathematics, Cartography and Cryptography. In the latter field he wrote "De Componendis Cyfris", a pioneer work in cryptography: it contains the first known frequency table and the first polyalphabetic system of coding by means of his cipher wheel. Alberti undertook this study, of obvious importance to the papacy (exchanging secret messages which cannot be understood by a third party is indeed fundamental in diplomacy!) at the request of a friend who was a papal secretary. This important booklet was published only in 1568 and it is clear why!

Cryptography requires a logical reasoning and applies some mathematical ideas, and presently is a branch of (applied) Mathematics. During Alberti's time it seems such an idea was not so common. Anyhow, for him Mathematics was a fundamental element in human society and provided precious instruments to the development of both arts and technology.

2. The cipher wheel

The encryption of a message from a plain text requires replacing each of its letters by another one according to some given rule which, when inverted, allows its decryption. A cryptosystem is called monoalphabetic if each letter is always replaced by the same different letter. Such a system is also referred to as a monoalphabetic substitution cipher, whereas a polyalphabetic substitution cipher is one in which a letter is replaced by another one according to its position in the plaintext too. Therefore, the concept of permutation (substitution) plays a fundamental role in cryptography. Let S be a set of symbols (often a set of positive integers). A permutation of S is just a rearrangement of the elements of S. E.g., 3,5,4,1,2 is a permutation of 1,2,3,4,5.



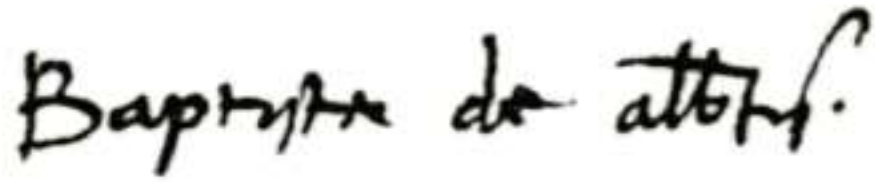
Alberti's cipher wheel provides varying permutations of the letters of the alphabet by means of a mechanical device, the cipher wheel. Such a device consists of two concentric disks having different diameters. each of which is subdivided into 24 equal sectors defining 24 boxes. Two copies of the wheel are needed, one for the sender of the message and the other one for the receiver. The boxes on the disks, both the big one and the small one, contain the letters of the alphabet. On the bigger disk the letters of the alphabet are in their natural order and in capitals. The letters H, K, Y, W and J are skipped , but the digits 1,2,3,4 are included, after Z. Such digits will be used to change the key and so ensure greater secrecy. On the smaller disk all lower case letters are inserted in the boxes in any random order; h, k, y are included and the symbol & is added (it denotes the Latin "et"). Note that u and v (U and V) are both in the same box on both disks. This is due to the fact that during Alberti's time these two letters were considered equivalent. The two disks are fastened together at their coinciding centres so that the smaller one, which is used to encrypt the message. can rotate.

The sender and the receiver agree on a common key consisting of a pair of letters, one on each disk, which allows to start the encryption, and such a key must be exchanged in a secure way. Assume the key is the pair (A,c); so the starting position of the two disks is that of the picture. To encrypt a message the sender shall

(i) eliminate the blanks between words, the accents and all possible punctuation; remove all H, K, replace W by V, and J, Y both by I; replace all double letters by a single one; insert by some random choice and in some random order the digits 1 to 4 in the message.

(ii) With each letter of the plaintext on the fixed disk (the bigger one) the corresponding letter on the small disk (the one which rotates) is associated till a

digit is found. The lower case letter corresponding to this digit (say q corresponding to 4) provides the new key (the initial key was (A,c), the new one will be (A,q)), and so on.



Example
Original plaintext: HALLE IS A BEAUTIFUL CITY Plaintext
ready for encryption: ALE4ISA1BEAUTI3FUL2CITI Encrypted
message: **czdqpoqlhqluybeix&okapa**

The decryption of a message just reverses the encryption process, as the following example shows.

Assume the encrypted message is

sfzefqqfxkmohihuy

and the agreed on key is again (A,c), which gives the initial position of the two disks. The lower case letters of the encrypted message are read on the small disk and we find

s = S,
f = I, z
= L, e =
V, f = I
q = 4

which gives
Silvi4

The digit 4 corresponds to q and the new key is (A,q), so that q = A,

x = O,
k = V,
m = E,
o = S h
= 2

hence

SILVIA LOVES 2.....

and proceeding as before, the recovered plaintext is

SILVIA LOVES CATS

3. Cryptography nowadays

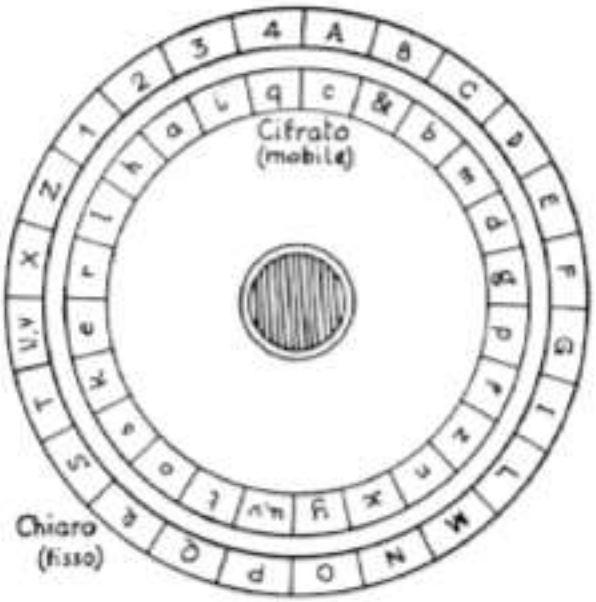
Leon Battista Alberti's cipher wheel provides a polyalphabetic cryptosystem which consists of an encrypting device, the wheel, and a private or symmetric key. The latter is known to sender and receiver only and must be transmitted through a secure channel so that no unauthorised person can get hold of it. Similar devices have been used till World War I. Afterwards, such devices became more sophisticated and the cipher machines employed during World War II used both mechanical and electromechanical devices which provided sequences of cipher wheels. Hence, sequences were used of different permutations both of the plain text elements and sets of such elements. When computers became well spread, programs replaced cipher devices. Such programs perform the required permutations both of letters and of blocks of the plain text. Again a private key is used which is usually broken up into subkeys each of which is employed in some step of the encryption. A well known example of such a cryptosystem is DES (Data Encryption Standard) which is still widely used. DES is a symmetric key cryptosystem and the same key is used both for encryption and decryption. The fact that such a key must be exchanged via a secure channel suggested (1976) the idea of a public key cryptosystem. This means using different keys for encryption and decryption so that the key needed to send a message to some user can be made public. This user will be the only one able to decrypt the message by his own private key.

Public key cryptosystems are constructed exploiting some mathematical problem which is considered unsolvable. Here unsolvable means that the solution requires an enormous computational effort and a very long time. One of the most popular public key cryptosystems is RSA (after the Mathematicians who introduced it: Rivest, Shamir and Adleman). Here the mathematical problem is that of factorising a positive integer which is the product of two distinct big primes. Note that big means an integer of several hundreds of decimal digits. Public key cryptosystems are employed for exchanging symmetric keys to be used in cryptosystems such as DES. for digital signatures, protection of credit cards and other smart cards.

4. Build your own cipher wheel

If you look at the picture, you will realise that it is easy to build an Alberti's cipher wheel. And you will need two identical copies of it: one for you and one for your friend who must be able to decrypt the messages you send him/her.

Take some cardboard, draw a bigger disk and a smaller one; cut them out and fasten them together in the middle (the centre!) in such a way that the smaller one can rotate. Divide both disks into 24 equal sectors (15 degrees each), and write the capital letters on the big disk in their natural order (see picture for the missing letters and the digits); write the lower case letters on the smaller disk in any order you like (see picture for missing letters) and use the same order on both copies of your cipher wheels.



Bibliography

Leon Battista Alberti (a cura di Augusto Bonafalce), *De componendis cyfris* , Torino,

Galimberti , 1998

P. Ferragine,F. Luccio, *Crittografia. Principi, algoritmi, applicazioni.* Torino, Bollati Boringhieri 2001

E. Garin, *Studi su Leon Battista Alberti* , Bari, Laterza 1976

D. Kahn, *On the originof polyalfabetic susbtitution,* ISIS (256)1980, pp. 122-127

S. Singh, *Codici e segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet,* Milano, Bur, Saggi 2001

G. Wolff, *Leon Battista Alberti als Mathematiker,* Scientia LX 1936 pp.553-556

Wilma Di Palma

Historician of Mathematics, mathematical Museologist and Scientific Curator of Mathematical Museum of Rome "I Racconti di Numeria"

Many thanks to professor Marialuisa J. de Resmini to have helped me in this English version.

Reports on History of Mathematics

Aus der Serie Reports on (Didactics and) History of Mathematics des Instituts für Mathematik (bis 2006 des Fachbereichs für Mathematik und Informatik) der Martin-Luther-Universität Halle-Wittenberg sind hier die der Geschichte der Mathematik in Wittenberg und Halle gewidmeten Hefte aufgelistet.

2008-13 T. Krohn: *Über die Schrift „Prodromus Conjuntionis Magnae, anno 1623. futurae. Das ist: Kurtzes und Einfeltiges, doch in Gottes Wort und der Astrologischen Kunst gegründets Bedencken von dem grossen Cometstern, der in abgewichenem 1618. Jahre im Novembri sich erst recht sehen lassen* [...]“ von Erasmus Schmidt (1570-1637), Professor für Mathematik an der Wittenberger Universität.

2008-08 M. Goebel, C. Schlensag: *Hans Brandes (1883–1965), Promotion in Halle – Lehrer in Braunschweig.*

2008-03 G. Warnecke: *Schulen und Schulverläufe bei Julius Plücker (1801-1868) und seinem Studenten August Beer (1825–1863) in einer Gesellschaft im Prozess grundlegender Äderungen, Teil II.*

2008-02 G. Warnecke: *Schulen und Schulverläufe bei Julius Plücker (1801-1868) und seinem Studenten August Beer (1825–1863) in einer Gesellschaft im Prozess grundlegender Äderungen, Teil I.*

2007-24 M. Bismarck, S. Schmerling: *Felix Bernstein: Ein ehemaliger Privatdozent der Vereinigten Friedrichs-Universität Halle-Wittenberg.*

2004-03 G. Warnecke: *Julius Plücker (1801-1868) in der philosophischen Fakultät der Universität Halle (07.11.1833-25.09.1835).*

2004-02 W.H. Schmidt: *Wenceslaus Johann Gustav Karsten (1732-1787). Von Neubrandenburg nach Halle – Bewerbungen, Beziehungen, Berufungen.*

2003-01 R. Tobies: *Mathematik-Promovierende an der Universität Halle im Vergleich mit Promovierenden an anderen Orten, 1907 bis 1945.*

2002-19 M. Goebel, Ka. Richter, Ku. Richter (Hrsg.): *Aspekte der Mathematikgeschichte in Halle.*

2002-05 S. Schmerling: *Albert Wangerin und August Gutzmer: Gedanken und Gedenken aus Anlaß der Neuanbringung ihrer Plaketten.*

2002-04 M. Goebel, E. Malitte, Ka. Richter, H. Schlosser, S. Schöneburg, R. Sommer: *Der Pantograph in historischen Veröffentlichungen des 17. bis 19. Jahrhunderts.*

2000-14 M. Goebel: *Bibliographie zur Geschichte der Mathematik in Wittenberg und Halle. 1. Fassung vom 20. Juni 2000.*

2000-13 V.R. Remmert: *Gustav Doetsch (1892-1977) in Halle, Stuttgart und Freiburg.*

2000-05 A. Koch: *Die Spezialklassen für Mathematik und Physik an der Martin-Luther-Universität Halle-Wittenberg.*

1999-21 H. Göpfert: *Carl Johannes Thomae (1840-1921) – Kollege Georg Cantors an der Universität Halle.*

1999-10 H. Donner: *Frieda Nugel: Die erste Doktorandin der Mathematik an der Universität Halle.*

1999-04 S. Schmerling: *August Gutzmer: Der Nachfolger Georg Cantor's an der Universität Halle.*

Es sei auf das Virtuelle Museum zur Geschichte der Mathematik in Wittenberg und Halle hingewiesen: `http://www.mathematik.uni-halle.de/history`.