Interactive tools for Mathematics learning related to the Cryptography

Abstract:
Education is very important nowadays. The researches in education are increasing year by year. This enhancement of the researches are the important aspect in the development of new educational methods techniques. Nowadays, the information society in our region needs wider educational spaces supported by the internet connection that provides a good tool to use educational technologies using online applications. Indeed, interactive tools give us privileges to have access to a huge amount of information in a multi-sequential way by using specifically suitable tools for the learning of a specific knowledge. These interactive tools have many advantages for learning mathematics. In our case, we present an interactive tool to show the main applications of Modular Arithmetic in a brief theoretical environment.

Key-Words:
Modular Arithmetic, Interactive Tutorials, Hypertext, World Wide Web, e-learning.

1. Introduction

The most widespread uses of technology in education comes out in the form of learning interactive tools. Using these Interactive tools are a very good complement to traditional learning via notes, books, etc [1]. There are a lot of studies, research and development such as multimedia applications, online tutorials and web application facilitate the way of educations using computer technology [2].

The reading, by exploration or navigation, of a hypertext is interactive. The reader makes visual sweepings and searches of fragments of interest. We recommend using textual or graphical tools that show in the screen and that allow the user to identify and to differentiate the contents of the hypertext [1]. When we use multiple media formats in our teaching, it will enrich experience of the users and improve the process of learning. Using this kind of multimedia application in an education stimulates students interest in a topic and enhances their motivation [3].

In the mathematical concepts and algorithmic procedures in the classroom is often difficult to describe. When the lecturer can explain the topic with different coloured chalks and explaining around the picture in the board or teaching using a well prepared slides presentations, the students can understand little more than static explanations. In this sense, using a good graphic interface environment will surely be a helpful for a better understanding of the mathematic concepts or how we can implement the algorithms [2].

During the last years, visualization software tools are increasing and becoming very popular and used in the education purpose, as a lot of publications have been done in educational conferences and journals.

We are working in Interactive tools four years ago, Interactive tools are being used by lecturer on the class lectures and students when they want to learn by themselves.

In this paper we are going to present our experience on using these Interactive tools for mathematics learning in the teaching and learning ways. We will also analyze the main requirements for these Interactive tools should carry out to be helpful for both lecturers that are not coming from computer area and the students in the first topic and we will present the advantages of these Interactive tools for mathematics learning that provide in learning processes [2].

Our objective is the development of interactive tools for Mathematics learning related to the cryptography to be used both by lecturer in the class and by students when they want to learn by themselves.

The use of this kind of tools in the class allows to visualize concepts, as well as to show a great number of examples in little time. The saved time can be used to do active learning activities.

2. Optimization of students' study time

When the students look up things of their own interest, they will find using the modern technology is very handy. In this case, the teachers should take improvements of this fact and should try to prepare for them such multimedia material which will optimize their study time. By creating this multimedia application, it will let students' study more effective, time efficient and explaining the topics will be more understandable [4].

We often lay stress on applying some principles when we teach a topic, so we can make sure that students have fully understand the explained topic matter.

Motivation to the topic

We used to use puzzle when we want to motivate a given topic. The students try to solve it, then discuss the solutions and after they explain the proper topic matter, we compare their solutions with an ideal solution based on the explained matter.

Teaching in contexts

We encourage students to think about any problem more than usual. By comparing the different attitudes, the students can get deeper into the problem and to understand it. In order to improve their view of discussed topic matter and deepen their awareness of it, we try to illustrate a particular problem with real life examples. We used to ask them to give their own examples that describe the topic to make sure that the topic is understandable.

Visualization of the particular issue

Demonstration and visualization make the topic much clearer and understandable. “Students need images and visualization in addition to words. Science learning is about creating images in mind, and teaching should support such image formation.“[4] We should use created appropriate multimedia applications as a complement of our lecturer.

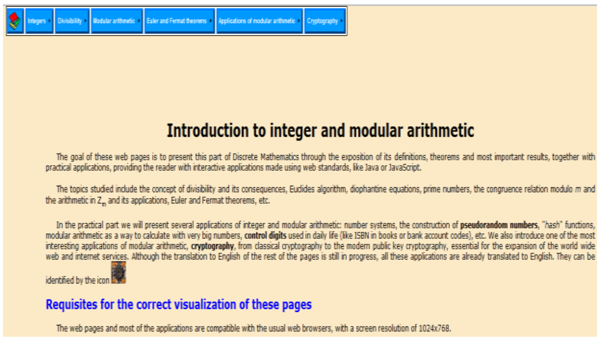
Increase of students’ self preparation

We try to prepare the material for students' self preparation to force them to study regularly and come ready to the class that can be run smoothly and more efficiently, like a discussion or consultation.

3. Description of interactive tools

With appearance of computer sciences in the second half of the 20th century, Modular Arithmetic well known by the old Greek and Chinese mathematicians. They have found its best applications specially with the invention of public key crypto systems. This interactive tools focuses on its theoretical and practical aspects as well. A lot of examples are included in the tools. It has been implemented using web technologies[5].

The below figure shows the home page of the tools where the reader can access the different sections that we will describe later.



Introduction to integer and modular arithmetic

The goal of these web pages is to present this part of Discrete Mathematics through the exposition of its definitions, theorems and most important results, together with practical applications, providing the reader with interactive applications made using web standards, like Java or JavaScript.

The topics studied include the concept of divisibility and its consequences, Euclides algorithm, diophantine equations, prime numbers, the congruence relation modulo *m* and the arithmetic in Z_m and its applications, Euler and Fermat theorems, etc.

In the practical part we will present several applications of integer and modular arithmetic: number systems, the construction of **pseudorandom numbers**, "*hash*" functions, modular arithmetic as a way to calculate with very big numbers, **control digits** used in daily life (like ISBN in books or bank account codes), etc. We also introduce one of the most interesting applications of modular arithmetic, **cryptography**, from classical cryptography to the modern public key cryptography, essential for the expansion of the world wide web and internet services. Although the translation to English of the rest of the pages is still in progress, all these applications are already translated to English. They can be identified by the icon

Requisites for the correct visualization of these pages

The web pages and most of the applications are compatible with the usual web browsers, with a screen resolution of 1024x768.

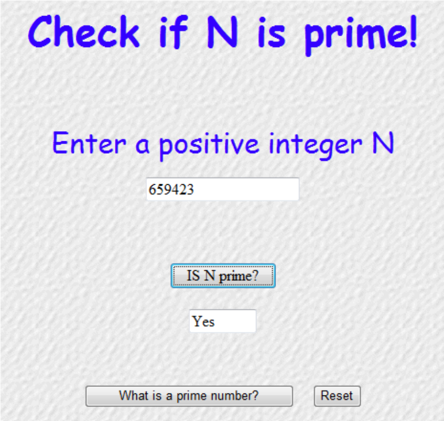
Figure 1. Home page of the tutorial.

The structure of the application is showing into the following pull-down:

- *Integers:* In this theoretical section we described the basic concepts about the integers and the induction principles.
- *Divisibility:* Divisors and multiples - Greatest Common Divisor (GCD) - Prime numbers. These theoretical concepts are complemented with applications to change the expression of numbers in decimal basis to other basis, and to calculate the GCD of two numbers using Euclid algorithm, or to find prime numbers in a given rank using the Sieve of Eratosthenes.
- *Modular arithmetic:* Congruence relation – Modular exponentiation. Modular Arithmetic is introduced from the congruence relation, showing next the methods to solve linear congruence equations and congruence systems. All this is also supported by some applications that shows the most common operations in Modular Arithmetic, the fast modular exponentiation and an application to solve systems of congruence equations.
- *Euler:* Primality tests and the usual methods to generate big prime numbers are also presented. A very interesting application of the notions studied so far is the cryptosystem RSA.
- *Applications of modular arithmetic:* Arithmetic with big numbers – Random numbers – Hash tables. The tutorial shows several very important applications of the calculus with congruencies in Computer Science, like the Arithmetic with very great numbers, the simple generation of random numbers in a computer science system.
- *Cryptography:* Introduction to cryptography – Information security – Cryptology – Public key and private key cryptosystems. The last part of the application is devoted to one of the most important applications of Modular Arithmetic nowadays: Cryptography. An historical introduction is included. Different cryptosystems, like Cesar cipher or poly alphabetical substitution are presented, along with their corresponding to practice coding with them. Finally, the most important public key cryptosystem, the RSA algorithm, is studied. This algorithm uses as encryption and decryption transformation the operation of modular exponentiation. Its security is based in the computational complexity that supposes the factorization of the product of two big prime numbers.

This application, written in dynamic HTML with Java script. We describe next some of the function:

3.1. Sieve of Eratosthenes: In order to illustrate the section dedicated to obtain prime numbers by means of the Sieve of Eratosthenes, small function has been made. Prime number is a natural number that has exactly two distinct natural number divisors: 1 and itself. In this system will show how to check if the number is prime or not. we enter the number then we press the button. it will print if it is prime.

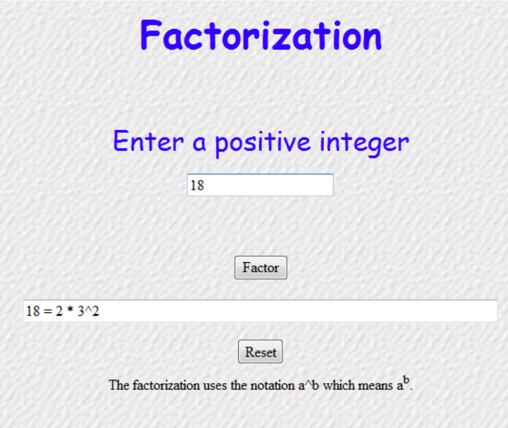


659423

Yes

Figure 2. Checking the prime number.

3.2. Factorization: It is the decomposition of an object (for example, a number, a polynomial, or a matrix) into a product of other objects, or factors, which when multiplied together give the original. In our system It will show the factorization of the positive integer number. We enter the number then we press the button. It will print the factors.



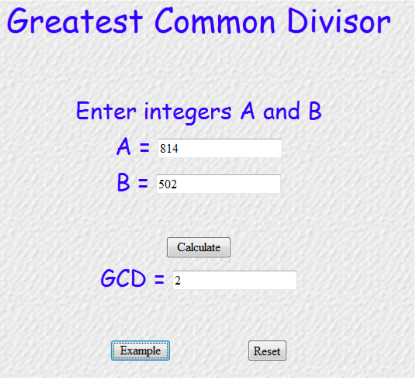
18

18 = 2 * 3^2

The factorization uses the notation a^b which means a^b.

Figure 3. Checking the factorization of number.

3.3. Euclid algorithm: This algorithm will help us to find the Greatest Common Divisor (GCD) which is two or more non-zero integers. It is the largest positive integer that divides the numbers without a remainder. This application shows the steps followed in Euclid algorithm to find the greatest common divisor (GCD) of two positive integers a and b. Moreover, the system computes a solution for the Diophantine equation aX + bY = gcd (a,b).



A = 814

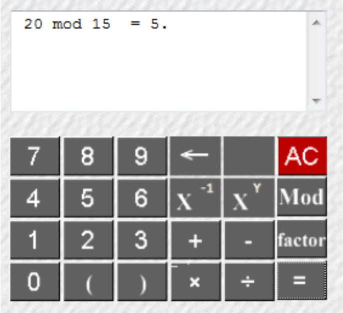
B = 502

GCD = 2

Figure 4. Checking the GCD of two numbers.

There are two text fields to enter the numbers whose greatest common divisor we want to compute. There is an activation button to tell the system to begin the execution of the algorithm from the entrances indicated in the text fields. Finally, there is an output text window to show the greatest common divisor of a and b, and the particular solution obtained for the diophantine equation aX+bY = gcd (a, b).

3.4. Modular Arithmetic: This section designed to show how to do the more common operations in Modular Arithmetic. The user must write a number and press mod and the write the mod number. The system will print the result.



```
20 mod 15  = 5.
```

Figure 5. Calculation the modular arithmetic.

4. Conclusions and future work

There are a lot of researches comparing the effectiveness of online learning and of face to face learning, researchers haven't demonstrated any significant difference. We found a lot of studies that have proved no significant differences between exam results of online students and those of face to face students [6], [7], [8]. However, there are cases in which online learning is reported to be more effective than face-to-face learning [9], while some research findings revealed that face-to-face learning is more effective than online learning [10]. These make us think that the best option is to use graphical and interactive tools in two ways. On one hand, these tools help the teacher in the classroom, while on the other hand, the students can work and experiment with them making their own examples, out the classroom. The didactical benefits of this interactive tutorial for Modular Arithmetic, according to our experience in teaching these mathematical concepts, are:

- It helps the student to learn the topic.
- It helps the teachers in their lectures by navigating through the examples and the applications implemented along the hypertext.
- They offer the student the opportunity to experiment, increasing interactivity.

In conclusion, the application designed and implemented abided by all the limitations of the project design specifications. The author hopes that this application will provide an enjoyable experience to the user and will benefit students in getting a further understanding in public key crypto-algorithms, (RSA encryption/decryption) and RSA signature [11].

This program can be further expanded so that it can provide a wider range of understanding for various types of cryto-algorithm. If there were more time, the application can be extended using large key lengths either 512-bits or 1024-bits.

References

[1] C. E. Iglesias, *et al.*, "Calculus b-learning with java tools," *WSEAS Transactions on ADVANCES in ENGINEERING EDUCATION*, pp. 295-305.

[2] M. G. S. Torrubia, *et al.*, "Pedagogical impact of Interactive Tutorials in Visualization and Learning of Mathematical Concepts in Computer Science Curricula," 2006.

[3] S. Encheva and S. Tumin, "Multimedia Factors Facilitating Learning," *WSEAS Transactions on ADVANCES in ENGINEERING EDUCATION*, vol. 4, pp. 203-209, 2007.

[4] E. Milkov "Multimedia applications and their benefit for teaching and learning at universities," *WSEAS Transactions on Information Science and Applications*, vol. 5, pp. 869-879, 2008.

[5] C. E. Iglesias, *et al.*, "Interactive tools for Discrete Mathematics e-learning," *WSEAS Transactions on ADVANCES in ENGINEERING EDUCATION,* pp. 97-103.

[6] R. Carlisle, "A Four Year Study Comparing English Classes Online, via Television, and Face-to-Face," *California State University,* 2002.

[7] A. R. Leasure, *et al.*, "Comparison of student outcomes and preferences in a traditional vs. World Wide Web-based baccalaureate nursing research course," *Journal of Nursing Education,* vol. 39, pp. 149-54, 2000.

[8] S. Street and A. Goodman, "Some experimental evidence on the educational value of interactive Java applets in Web-based tutorials," 1998, pp. 94-100.

[9] J. L. Johnson, *Distance education: The complete guide to design, delivery, and improvement*: Teachers College Pr, 2003.

[10] B. W. Brown and C. E. Liedholm, "Can web courses replace the classroom in principles of microeconomics?," *The American Economic Review,* vol. 92, pp. 444-448, 2002.

[11] L. Pham, "EDUCATIONAL SOFTWARE TOOL FOR A CRYPTOGRAPHIC LABORATORY."