Interactive Web Tutorial for Integer and Modular Arithmetic and its Applications

LUIS MIGUEL CARMONA COLLADO
CARMEN ESCRIBANO IGLESIAS
ANTONIO GIRALDO CARBAJO
MARÍA ASUNCIÓN SASTRE ROSA
Applied Mathematics Department – Computer Science Faculty
Polytechnic University of Madrid
Campus de Montegancedo – Boadilla del Monte – 28660 Madrid
SPAIN

Abstract: - Nowadays, TICs (technologies for informatics and communication) provide a very positive aid to the learning tasks. Interactive tutorials provides access to a big amount of information in a multi-sequential way, by using specifically designed Java applets suitable for the learning of a specific knowledge. Due to these facts, the use of these tools has many advantages for learning mathematics. In this sense, we present here a hypertext developed to show different applications of Integer and Modular Arithmetic in a brief theoretical environment.

Key-Words: - Modular Arithmetic, Interactive Tutorials, Hypertext, Java Applets, World Wide Web, RSA Cryptosystem.

1 Introduction

The reading by exploration or navigation of a hypertext is multi-sequential and interactive. The reader makes visual sweepings and searches of fragments of interest. It is recommendable to use textual or graphical tools that appear in the screen and that allow the user to identify and to distinguish the contents of the hypertext. Navigation has replaced linear reading, the information is a space to travel, a path to explore.

On the other hand, Modular Arithmetic, already well-known by the old Greek and Chinese mathematicians, has found its greatest applications in the second half of the 20th century, with the appearance of Computer Science. In particular, it has obtained a great relevance with the invention of public key crypto-systems.

The work that we present here is the elaboration of a hypertext, including several Java applets, to be used by teachers on the classroom lectures and by the students when learning by themselves. This hypertext summarizes the subject "Integer and Modular Arithmetic". This is part of the syllabus of the course "Discrete Mathematics", taught in the first semester of Computer Science at the Polytechnic University of Madrid. The hypertext includes all the definitions, theorems and the most important results, along with some practical applications. For the latter, we have designed several interactive applets that allow the reader to experience a high degree of interactivity, offering him the freedom to generate its own examples. These applets are made using programming standards for the World Wide Web, like Java or JavaScript.

We have been working since many years ago, developing interactive tools to help the teacher to present and display, in an animated and interactive way, many mathematical notions and algorithms in the classroom. These tools can be also used by the students through the web page of the Department to experiment with the contents of the various courses taught by us in a virtual way.

2 Objectives

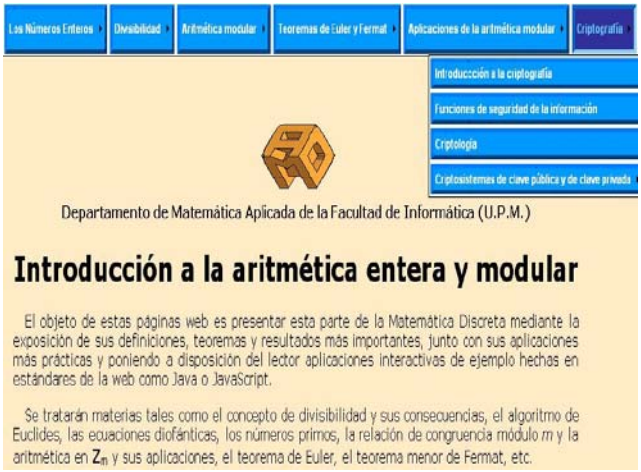
The main objective of this work is to develop interactive tools for the subject "Integer and Modular Arithmetic" to be used both by teachers on classroom lectures and by students when learning by themselves. As most mathematical subjects, this is difficult for students. To make it as friendly and attractive for students as possible, we have given special attention to the following properties of these tools:

- A graphical interface for the hypertext which can be easily handled by the user. It allows the visualization of the contents and the organization of the information in an immediate way through pull-down menus. One of our goals is that the different applications which are presented in the tutorial can be easily and quickly found within each section.
- Fast access to bibliography, books and numerous related web pages.
- Implementation of didactic applets for the most relevant algorithms of Integer and Modular Arithmetic, which have provided many important applications, most of them widely used nowadays. These applets are immersed in a theoretical framework in which the several notions and results are presented. Therefore, as we pretended, the user can interact with the tutorial, so that its use is more attractive and interesting.
- Inclusion, following this didactic direction, of historical references and anecdotes about some of the excellent mathematicians who helped to develop this subject. Those are referred in the hypertext with an icon.
- Accessibility from the web page of the department, as additional documentation for the course "Discrete Mathematics". This will be also integrated in a b-learning moodle context.
- Design of the applets using programming standards for the World Wide Web, to avoid incompatibilities.
- Facility to include new functionalities and algorithms in the future, if desired.

3 Description of the interactive tutorial

This interactive tutorial focuses in theoretical as well as in practical aspects. Numerous practical examples are included, as well within the texts as in the form of interactive applications for the Web. These applications have been implemented using technologies characteristic of the Web, in the form of Java applets or as dynamical web pages using Javascript.

The next figure shows the page from which the reader can access the different sections that we describe next.



The theoretical part begins with the basic notions about the integers and the induction principle, concepts like divisibility and prime numbers, Euclid algorithm and Diophantine equations. These theoretical notions are complemented with applications, in the form of applets, for changing the expression of numbers in decimal basis to other bases, to compute the greatest common divisor of two numbers using Euclid algorithm, or to find prime numbers in a given rank using the Sieve of Eratosthenes.

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 like an applet that shows the most common operations in Modular Arithmetic, the fast modular exponentiation and an application to solve systems of congruence equations.

In the next section, the units of Z_m, Euler function and Euler theorem, and Fermat little theorem are briefly introduced. 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.

The tutorial shows several very important applications of the calculus with congruencies in Computer science, like the Arithmetic with very great numbers, the hash tables used in programming when it is necessary to quickly find a data registry in a very great table, the simple generation of random numbers in a computer science system (that is determinist by nature), or the control digits that are used in systems widely used in the daily life (the Spanish ID or DNI, the codes of client accounts in banks, or the ISBN, an identification code for printed books). An applet to

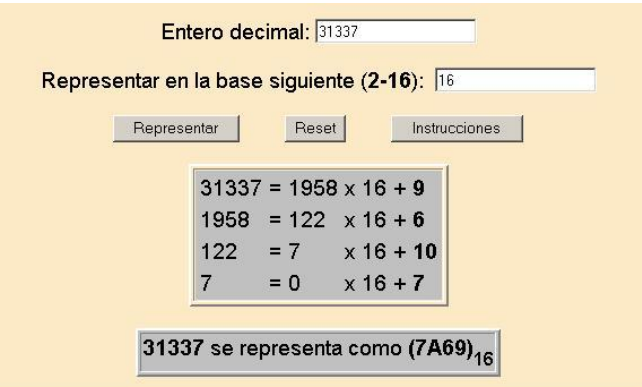
generate pseudorandom numbers and another to verify control digits, are included here.

The last part of the tutorial is devoted to one of the most important applications of Modular Arithmetic nowadays: Cryptography. An historical introduction is included. Different cryptosystems, like Cesar coding or the coding by poly-alphabetical substitution are presented, along with its corresponding applets to practice coding with them. Finally, the most important public key cryptosystem, the RSA algorithm, is studied. This algorithm uses as coding and decoding 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.

We describe next some of the applets.

3.1 The application “change of basis"

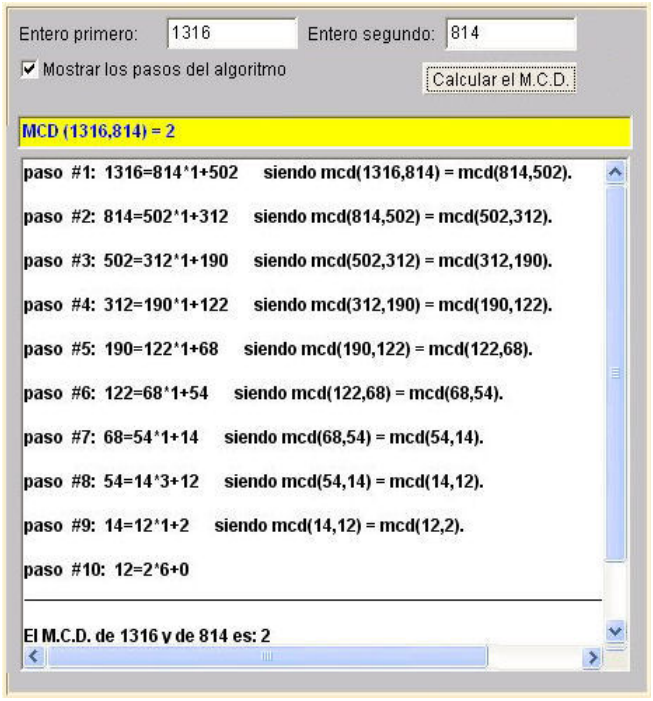
This application, written in dynamic HTML with Javascript, shows how to convert a nonnegative integer from decimal basis to any other basis. Any basis between 2 (binary representation) and 16 (hexadecimal) can be chosen for the conversion. For the cases of basis greater than 10, the letters A to F are used, as usual, to represent the digits 10 to 15. There are two text fields to enter the number in decimal basis and the new basis in which it is desired to express the number. Aside from both text fields, there are three buttons to indicate the desired action. The button “To represent” makes two text areas appear in the lower half of the user window. Those are the exits of the interface. The first area displays the process of conversion, and the second shows the final results, i.e., the representation of the input integer in the desired basis. The “Reset” button erase the contents of the text fields and the two output areas. The button “Instructions” opens a new navigator window with the instructions to use the program.



3.2 Euclid algorithm

This Java application shows the steps followed in Euclid algorithm to find the greatest common divisor (gcd) of two positive integers a y b. Moreover, the applet computes a solution for the Diophantine equation aX + bY = gcd (a,b)

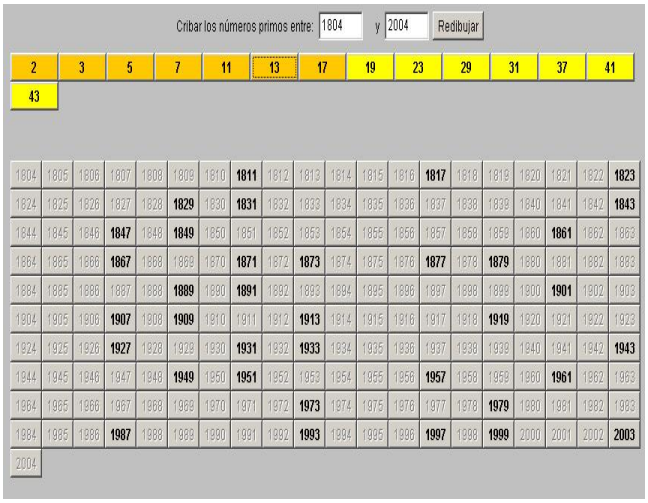
There are two text fields to enter the numbers whose greatest common divisor we want to compute and a box to indicate if the applet must show or not the different steps in the execution of the algorithm. There is an activation button to tell the applet to begin the execution of the algorithm from the entrances indicated in the text fields. Finally, there is an output text window to show the error messages or, if no error has been found in the input data, the different steps in the execution of the algorithm (if the corresponding box has been checked), the greatest common divisor of a and b, and the particular solution obtained for the diophantine equation aX+bY = gcd (a, b).



3.3 The Sieve of Eratosthenes

In order to illustrate the section dedicated to obtain prime numbers by means of the Sieve of Eratosthenes, two applets have been made. The second one allows to look for (by means of the Sieve of Eratosthenes) all the prime numbers in a prescribed interval of integers (the maximum interval size is 500, for reasons of spatial representation in the screen) contained in [101, 9999].

The applet interface is as follows. The text windows to input the end points of the interval where to look for prime numbers are in the upper part of the panel. In the following line there is a line of buttons corresponding to all prime numbers lower or equal than the square root of the upper end of the interval. Initially, all these buttons are active (yellow). When one of these buttons is pressed by the user, that button passes to a inactive state (orange) and all their multiples disappear from the table, as if they had been "sieved" from the table.



3.4 The cryptosystem RSA

This applet allows to encrypt or to sign a short text message using the algorithm RSA. The applet is divided in three areas:

· Area 1 – Generation of the pair of keys RSA

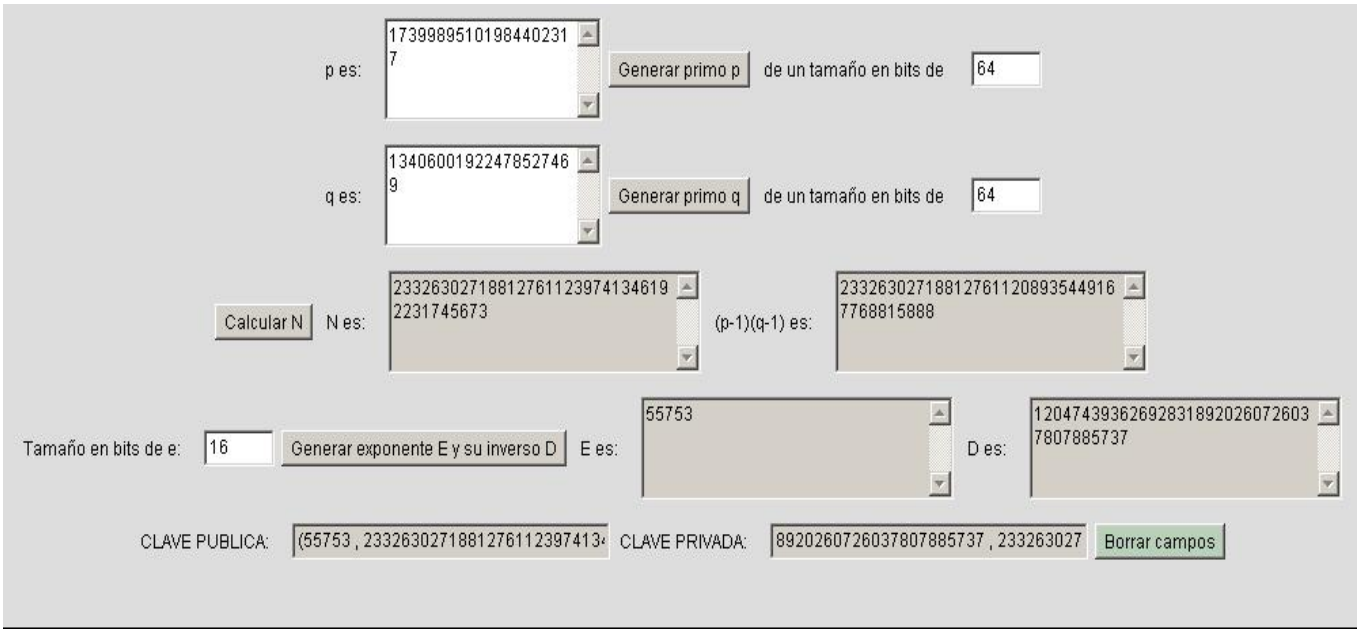
First, the pair of keys (public and private) for the user has to be generated. For this, the applet asks for a pair of prime numbers p and q. The application itself can generate these two prime numbers. Then, the values of the module n=p·q and of the public exponent E, which is generated randomly by the applet with the size in bits indicated by the user, are computed. The value of the exponent D is calculated automatically by the applet. These values determine the public key (E,n) and the private key (D,n) with which the user can encrypt/decrypt and sign messages.

· Area 2 – Encrypting and signing the message

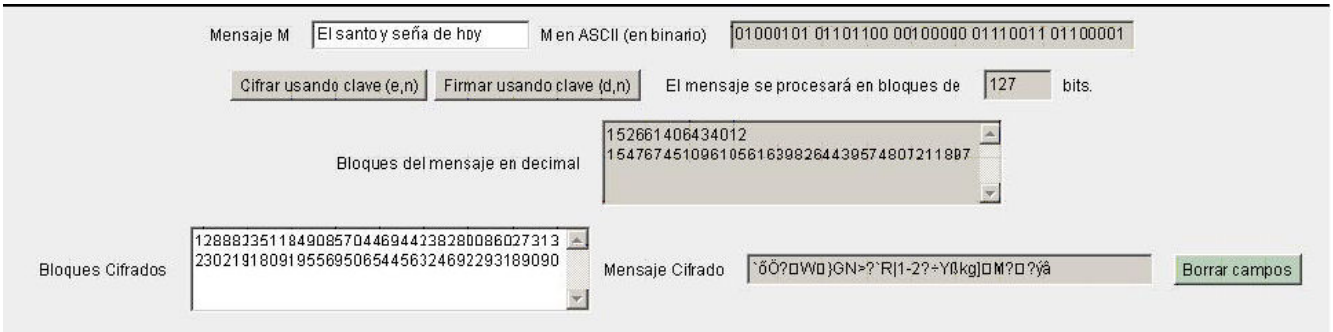
The message is written in the designed text field and then the "encrypt" button has to be pressed. If the text is very long it will be encrypted by blocks.

· Area 3 – Decrypting the message and signature verification

Here the inverse process of the previous step is made. The numbers corresponding to the presumed encrypted message or to the presumed signature are introduced, and the modular exponentiation of the RSA algorithm is repeated using this time as exponent the private key (for decrypting) or the public key (for verifying the signature). In a real case, the verification of our signature would not be made by us, but by the receiver of the resume of our signed message, who would verify it using our public key.



Area 1 of the applet RSA – Generation of the pair of keys



Area 2 of the applet RSA – Encrypting and signing the message

4 Conclusions and future work

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 study the course.
- 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 general, interactive tutorials including Java applets are very good aids for learning mathematics, as they improve comprehension, engagement, memorization and the satisfaction of the students, as well as the interest and motivation amongst pupils when the teacher makes use of them.

Finally, as a future work, we continue developing interactive tutorials in different areas of Mathematics related to Computer Science (we have already made tutorials for some parts of Infinitesimal Calculus, Dynamical Systems, Fractal Geometry, Image Processing, …). We intend also to elaborate interactive books.

References:

[1] A. Giraldo, Aritmética Entera y Modular, http://www.dma.fi.upm.es/docencia/primerciclo/matdiscreta/12M/TeoriaAritmetica.pdf /.

[2] T.L. Naps, G. Rößling, et al, *Exploring the Role of Visualization and Engagement in Computer Science Education.* Inroads - Paving the Way Towards Excellence in Computing Education. 35, 131-152, ACM Press, 2003.

[3] J.C. Orós, *Diseño de páginas Web interactivas con JavaScript*. RA-MA 1999.

[4] K.H. Rosen, *Discrete Mathematics and its Applications*, Mac Graw-Hill, 2007.

[5] M.G. Sánchez Torrubia, M. A. Sastre Rosa, V. Giménez Martínez, C. Escribano Iglesias *Pedagogical impact of Interactive Tutorials in Visualization and Learning of Mathematical Concepts in Computer Science Curricula,*. Proceedings Conference on Informatics Education in Europe, Montpellier, November 2006.

[6] M.G. Sánchez Torrubia, M.A. Sastre Rosa, V. Giménez Martínez, C. Escribano Iglesias, *Visualization on Learning Mathematics Concepts for Engineering Education*, The 4th WSEAS / IASME International Conference on Engineering Education (EE'07), Crete, Greece, July 2007.

[7] S.Street, A.Goodman, *Some experimental Evidence on the Educational Value of Interactive Java Applets in Web-based Tutorials*, Proceedings of the 3rd Australasian Conference on Computer Science Education, ACM, 94-100, 1998.

[8] *Introducción a la aritmética entera y modular*, http://www.dma.fi.upm.es/java/matematicadiscreta/aritmeticamodular/.

[9] *FAQ "La criptografía de hoy" de RSA Security* http://www.rsasecurity.com/rsalabs/node.asp?id=2152.

[10] *Revista independiente on-line sobre privacidad y seguridad en Internet*, http://www.kriptopolis.com.