

DISCRETE MATHEMATICS AND DIGITAL TECHNOLOGY

CANAVELLI, Juan Carlos ^{1,2}, GAITÁN, María Mercedes ^{1,2}, VAIRA, Stella Maris ^{1,3}

jcanavelli@frp.utn.edu.ar

mgaitan@frp.utn.edu.ar

svaira@fcb.unl.edu.ar

¹Facultad Regional Paraná Universidad Tecnológica Nacional - Almafuerde 1033 - (3100) Paraná - Entre Ríos.

²Facultad de Ciencia y Tecnología Universidad Autónoma de Entre Ríos - Oro Verde - (3100) Paraná - Entre Ríos.

³Facultad de Bioquímica y Ciencias Biológicas Universidad Nacional del Litoral - Ciudad Universitaria - Paraje EL POZO - (3000) Santa Fe - Santa Fe.

ARGENTINA

Key Words: Education, Discrete Mathematics, Technology, Elementary Number Theory.

Summary

One of the characteristics of this century is the advance of technology, mainly digital technology. We are surrounded by computers, we surf Internet, use CDs, DVDs, MP3s, MP4s, iPods, digital cameras, cellular phones with GSM technology and many others. Some teachers of Mathematics feel a deep emotion being aware that all these modern technologies apply knowledge from a very old branch of our discipline: the Elementary Number Theory. This supports many of the concepts developed by classical or modern Algebra. However, and because of strong reasons, this theory is integrated in courses so called **Discrete Mathematics**.

The objective of this paper is consider briefly what is Discrete Mathematics and how support some of the modern information and communication technologies. Also we stand out how important it is for adolescents and youngsters of this XXI Century know these concepts, because they use their applications daily with enthusiasm and competence. Meanwhile they reject, out of ignorance, the discipline which originated them. When students become aware that Math is in everyday life now, more than ever, decide to make an effort to learn it. We know the truth underlying the old saying: *“When there’s a will there’s a way. (Otherwise, there are always excuses)”*. Finally there are ideas on the implications of these facts for those who are teachers of Mathematics today.

Resumen

Una de las características de este siglo es el avance de la tecnología, en particular la tecnología digital. Estamos rodeados por computadoras, navegamos en INTERNET, usamos CD, DVD, MP3, MP4, iPod, cámaras digitales, teléfonos celulares con

tecnología GSM, etc. Algunos docentes de Matemática sentimos una profunda emoción al advertir que todas estas modernas tecnologías utilizan conocimientos de una rama muy antigua de nuestra disciplina, la Teoría Elemental de Números. Esta teoría fundamenta muchos de los conceptos desarrollados por el Álgebra, sea Clásica o Moderna. Sin embargo, poderosas razones la integran hoy, muchas veces, en los cursos de la llamada MATEMÁTICA DISCRETA. En este trabajo nos proponemos considerar brevemente qué es la Matemática Discreta, cómo se presenta en el fundamento de algunas de las modernas Tecnologías de la Información y de la Comunicación. También consideramos brevemente la importancia de que estas aplicaciones de la Matemática sean conocidas por los adolescentes y jóvenes del Siglo XXI, que las utilizan diariamente con entusiasmo y competencia, al mismo tiempo que muchas veces rechazan, por ignorancia, a la disciplina que les dio origen. Nuestra experiencia nos dice que cuando el estudiante advierte que, jamás como ahora, la Matemática impregna la vida cotidiana, se decide a hacer el esfuerzo que implica su aprendizaje. Y ya sabemos cuán cierto es el antiguo adagio: “*Cuando alguien quiere hacer algo, encuentra los medios. Cuando no quiere hacerlo encuentra la excusa*”. Terminamos el trabajo con una reflexión sobre las implicancias de estos hechos para quienes hoy somos docentes de Matemática, a la luz de la trascendencia de nuestra disciplina en el actual desarrollo tecnológico, y en consecuencia en el desarrollo económico y social de los pueblos.

1. Discrete Mathematics

What is Discrete Mathematics? We can answer this question looking to Mathematics or Mathematics Education.

From a mathematical viewpoint, Discrete Mathematics is the study of sets, finite or infinite, with certain structure. We can say that \mathbf{Z} (the set of whole numbers), is the paradigm of Discrete Mathematics.

Looking to the teaching of Mathematics, we must say that in the XX century (around 60s), it was noticed that future specialists in the field of Information Technology should acquire knowledge not included in the traditional Algebra and Differential and Integral Calculus. Therefore, new courses and textbooks turn up including very traditional topics (Elementary Number Theory, Combinatorial Enumeration, Graph Theory, Logic, Boolean Algebra, and Abstract Algebra (Abstract...?)), with more modern topics (Languages and Finite States Machines, Theory of Algorithms and Computational Complexity).

Ironically, it is said that courses on Discrete Mathematics should include all the themes needed by specialist of Information Technology, which are not covered by the courses on Calculus.

Another issue emerges: Considering that computers are discrete machines, how much knowledge of Continuum Mathematics should Information Technology specialists acquire...?

Due to its mathematical, pedagogical and technological relevance, we will discuss some considerations on Elementary Number Theory, including in Discrete Mathematics.

2. Review of the Concepts on Elementary Number Theory

It is known that concepts of Elementary Number Theory, such as natural numbers, appeared in the earliest times of history and in several cultures when people started to count. Then, the invention of zero meant great progress. In our civilization, the invention by the Hindus is of interest, although it should be mentioned that the Mayans had also reached that level of abstraction, surpassing the achievement of the Romans. Later in time the negative whole numbers were invented.

The Elementary Number Theory works only with whole numbers and the main topics are: Division Algorithm, Greatest Common Division, Diophantic Equations, Prime Numbers, Fundamental Theorem of Arithmetic, Congruence, Fundamental Theorems of Modular Arithmetic (The Chinese Remainder Theorem, Fermat's and Euler-Fermant's Theorems).

We should stop and comment the concept of **congruence** in the set of whole numbers. This concept is use in our daily lives when we work with hours (clock arithmetic). For example, if somebody sets off on a trip at 22h (or 10pm) and the trip lasts 10 hours, we know the traveler is arriving at 8h (or 8am) of the following day. Therefore, there is something very natural and strange at the same time happening: just looking at the clock and adding the departure time to the duration of the trip we obtain a number which is smaller than the former:

$$22\text{h or }10\text{pm (departure time)} + 10\text{h (duration of the trip)} = 8\text{h or }8\text{am (arrival time)}.$$

What happened...? Simply, hour 24 of a day coincides with hour 0 of the following day, and basically what matters each day are the hours from 0 to 23. It looks like irrelevant issue in the mix of these basic considerations. However, the idea behind, is the basic of modern technological realizations. For example, correction of errors that occur in transmission (cellular telephones, photographs of remote regions in space) or information storage (CDs, DVDs) even the confidentiality of information (e-commerce) and the identification of the sender of a message (the law of digital signature) use this concept.

We can turn now to more formal definitions and expressions.

If we agree that $n \mid m$ should be read: n divides exactly m , we say;

Definition: Let $a, b \in \mathbf{Z}$, and be $n \in \mathbf{N}$, with $n > 1$, then a is congruent to b module n if $n \mid a - b$

Notation: $a \equiv b \pmod{n}$

Example 1: If $n = 5$, results: $78 \equiv 43 \pmod{5}$, for $5 \mid 78 - 43$, because $5 \mid 35$ i.e. "5 divides 35", or we could also say that "35 is a multiple of 5"

$$\text{If } n = 24 \text{ then } 32 \equiv 8 \pmod{24}, \text{ since } 24 \mid 32 - 8$$

It immediately results that the congruent relationship in \mathbf{Z} is reflexive, symmetrical and transitive, i.e., it is an equivalence relationship. Therefore it induces a partition in the set of whole numbers, dividing it in classes of equivalence. We represent the quotient set as $\mathbf{Z}/n\mathbf{Z}$, or \mathbf{Z}_n (finite set of classes).

Example 2: With $n = 3$, it results: $[0] = \{ \dots, -9, -6, -3, 0, 3, 6, 9, \dots \}$

$$[1] = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$$

$$[2] = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$$

Therefore, the resulting set of classes is: $\mathbf{Z}_3 = \{[0], [1], [2]\}$

Remark 1: Notice that the representative numbers of the classes: 0, 1 and 2 correspond precisely to the remainders of the whole division by 3. For this reason, the terms “residual classes” are often used.

Remark 2: When there is no possibility of misunderstanding, it is common to represent classes without square brackets in their notation. From now we will in general use this convention, writing: $\mathbf{Z}_3 = \{0, 1, 2\}$. However, always remember that we are not working with numbers, but with sets of numbers (equivalence classes).

In these finite sets we will define the operations of addition and multiplication from the corresponding operations with whole numbers. Then, working in \mathbf{Z}_n , results:

$$[a] + [b] = [a + b] \quad \text{and}$$

$$[a] \times [b] = [a \times b]$$

Looking to minimize the number of symbols in use, we use + and \times with two very different meanings:

In $[a] + [b]$ and $[a] \times [b]$; + and \times refer to the new operations we are defining; while in $[a + b]$ and $[a \times b]$; + and \times refer to the well-known operations of whole numbers, i.e. the usual addition and multiplication.

We will now construct tables for these operations.

Example 3: In $\mathbf{Z}_3 = \{0, 1, 2\}$ results:

Table of the sum

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table of the product

\times	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Remark 1: Notice that $(\mathbf{Z}_3, +, \times)$ is a commutative ring.

Remark 2: In a deeper analysis, we also notice that it is a finite field because all elements different a zero can be inverted in a multiplication (the multiplicative inverse of 1 is 1, and of 2 is 2).

In fact, this finite field is an example of Galois field. Another notation used for representing it is $\text{GF}(3)$.

Somebody rightly said that it is important to think carefully about simple issues. Applying this principle to the case we are working with now, obviously we know what

happens with the GF(2) constructed with set $\mathbf{Z}_2 = \{0, 1\}$. The results are so simple that you can think it is a waste of time to even build these tables. See below:

Table of the sum

+		0	1
0		0	1
1		1	0

Table of the product

×		0	1
0		0	0
1		0	1

Therefore whoever underestimate this “simplicity” is completely wrong. The Galois field has a particular importance in the transmission and storage of information. In fact, all the information is transmitted or stored in chains of “zeros” and “ones” (bits) which operate element to element in \mathbf{Z}_2 . Mathematically, we are operating with k-uplas of bits, i.e., in the set $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \dots \times \mathbf{Z}_2$ (k factors), where in general the usual notation is not applied (parenthesis and commas) for k-uplas, but with sequences of “0” and “1”, e.g. 0001100, instead of (0, 0, 0, 1, 1, 0, 0).

Example 4: Suppose we work with 7-uplas. Then we can write:
 $0100111 + 1011101 = 1111010$

3. Activities Developed

Thinking that teachers are the core of the technological, economic and social development of the countries, the members of this group have participated in three updating courses:

- a) **DISCRETE MATHEMATICS I:** Mandatory to pre-service Mathematics teachers.

Objectives

The students are expected to:

- a.1 deepen their knowledge of concepts and methods of study of some of the structures of discrete mathematics.
- a.2 develop their ability in the use of logical reasoning, conjecture formulation and its rigorous analysis; proposal and problem solving.
- a.3 value the historical evolution of the concepts and methods studied.
- a.4 link contents developed with those of other fields of Mathematics.
- a.5 know current applications of Discrete Mathematics.
- a.6 appreciate the potential of modern technological resources and their possibilities in the teaching/learning process and some Mathematical applications.
- a.7 value the importance of Discrete Mathematics in the learning process at the initial levels.

Contents

Thematic Unit 1

Introduction. What is Discrete Mathematics? Elementary Number Theory: Divisibility of whole numbers. Division algorithm. Number Systems. Greatest Common Divisor. Linear diophantic equations. Prime numbers. Fundamental Theorem of Arithmetics. Pythagorean triples. Infiniteness of Prime Numbers. Distribution of Prime Numbers.

Thematic Unit 2

Congruences. Classes of congruences. Structure of the set of classes. Congruences with unknowns. Chinese Remainder Theorem. Fermat's Little Theorem. Perfect Numbers. Fermat-Euler Theorem. Applications in Cryptology. Classical Cryptosystems. RSA cryptosystem.

Thematic Unit 3

Combinatorial Principles. Problems leading to recurrence relations. Solution of some relations of homogeneous and non-homogeneous linear recurrence. Application of recurrence relations.

- b) **ARITHMETIC AND ALGEBRA SEMINAR:** Aimed to update in-service teachers.

Objectives

Attendants to this seminar are expected to:

- b.1 develop their ability in the use of logical reasoning, conjecture formulation and its rigorous analysis; proposal and problem solving.
- b.2 value the historical evolution of the concepts and methods studied.
- b.3 value the importance of these topics in Mathematics studies at any level.
- b.4 link contents developed with those of other fields of Mathematics
- b.5 know the current applications of these concepts to Information Technology
- b.6 appreciate the potential of modern technological resources in the teaching/learning process of Mathematics.
- b.7 enhance their keenness on problem formulation and solving.
- b.8 increase their appreciation of the precision and concision of mathematical language.

Contents

Divisibility of whole numbers. Division algorithm. Greatest Common Divisor, Euclides Algorithm. Linear diophantic equations. Prime numbers. Fundamental Theorem of Arithmetic. Pythagorean triples. Infiniteness of Prime Numbers. Distribution of Prime Numbers. Congruences. Classes of congruences. Structure of the set of classes. Congruences with unknowns. Chinese Remainder Theorem. Fermat's Little Theorem.

Fermat-Euler Theorem. Applications of the Elementary Number Theory in Cryptology. RSA cryptosystem. A current vision on primality and factorization. Groups. Groups and congruences. New formulation of the Chinese Remainder Theorem. Rings. Subrings and ideals in \mathbf{Z} . Homomorphisms. Polynomial rings. Fields. Finite fields. Applications.

- c) **THE ELEMENTS OF CRYPTOGRAPHY:** Intended for teachers, graduates and senior engineering students.

Objectives

On completion of this course, successful attendants are expected to:

- c1. know fundamental concepts of classical cryptography of secret key.
- c2. notice their weaknesses faced with powerful methods of current calculus.
- c3. understand the fundamental concepts and methods of the Elementary Number Theory.
- c4. be able to use specific software to solve the problems posed by this branch of Mathematics.
- c5. understand the application of Mathematics in some current cryptographic systems (RSA-ElGamal).
- c6. know other applications of Mathematics in modern cryptography.

Contents

Introduction to Cryptography and Cryptoanalysis. Classical Cryptography: historical remarks. Julius Caesar's System. Alberti and Vigenère. The Enigma Machine. Concepts of the Elementary Number Theory: Divisibility, congruences, modular arithmetics, the Chinese Remainder Theorem, Fermat's Little Theorem, Euler's ϕ function, etc. Modern Cryptography: Diffie-Hellman key exchange. The RSA System. ElGamal System. Digital signature and other current applications.

Also this group has participated in extension courses of topics related to this area of Mathematics.

4. Final Comments and Conclusion

New technologies offer excellent opportunities to motivate and deepen the teaching of several mathematical issues. Particularly the Discrete Mathematics challenge students to solve simple and complex problems and is the base of different mathematics concepts. Adding to a pedagogic value, this discipline has the honor to be the fundament of all digital modern technology. This fact gives it a unique value as motivator of the Mathematics learning for children and young people in the XXI century. So it is very important that teachers of Mathematics know Digital Signal Processing as well they deepen in the Maths aspects of it given the discrete mathematics the importance that deserve in this century.

Our experience teach us that even in the worse conditions, such us belong to a developing country, we can go in the right direction. Even the study of Differential and Integral Calculus can start with discrete concepts, as sequences and series of constants. In the frame of Mathematical Modeling, the Difference Equation (or Recurrence

Relations), should be study before the Differential Equation. We know the effort that means, but we are positive that it is our social responsibility.

Being argentinians it is hard to say that even in the XIX century, Domingo Faustino Sarmiento see the relevance of education in the society welfare, but we did not pay attention. In the “knowledge era” we can see he was right. It is our responsibility now, from the maths classrooms, to promote the economical and social development of our countries.

5. References

Becker, M. E.; Pietrocola, N. & Sánchez, C. *Aritmética*. Red Olímpica. Olimpiada Matemática Argentina. Buenos Aires. 2001.

Bor, Gil. *Introducción a la Teoría de Números*. Centro de Investigación en Matemática (CIMAT). Taller de Ciencia para Jóvenes. CICESE. Guanajuato, México. 2001

Conway, J. & Guy, R. *The book of Numbers*. Springer-Verlag. New York. 1996.

Gentile, E. R. *Aritmética elemental en la formación matemática*. Olimpiada Matemática Argentina. Buenos Aires. 1991.

Hardy, D. W. & Walter, C. L. *Applied algebra – Codes, Ciphers and Discrete Algorithms*. Prentice Hall. 2002.

Koblitz, N. *A course in number theory and cryptography*. Springer-Verlag. New York. 1994.

Lauritzen, N. *Concrete Abstract Algebra-From Numbers to Groebner Bases*. Cambridge University Press. Cambridge UK. 2003.

Niven, I.; Zuckerman, H.S. & Montgomery, H.L. *An introduction to the theory of numbers*, fifth ed. John Wiley & Sons Inc. New Cork. 1991.

Santaló, L. A. & collaborators. *Enfoques. Hacia una didáctica humanista de la matemática*. Editorial Troquel. 1994.

Singh, S. *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Doubleday. 1999. Electronic version available at: http://www.simonsingh.net/Code_Book_Download.html

Stein, W. *Elementary Number Theory*. Intended for Publication by Springer-Verlag 2004. Electronic version available at: <http://modular.math.washington.edu/ent/>

Zazkis, R. “Múltiplos, divisores y factores: explorando la red de conexiones de los estudiantes”. RELIME. Vol 4:1. pp 63-92. México. 2001.

Zazkis, R.; Campbell, S. *Number Theory In Mathematics Education. Perspectives And Prospects..* Lawrence Erlbaun Associates Publishers Mahwah, New Jersey – London. 2006.