An Active Learning Activity for the Construction of a Finite-Field Slide Rule for Undergraduate Students

An Active Learning Activity for the Construction of a Finite-Field Slide Rule for Undergraduate Students

Marco Abrate

An Active Learning Activity for the Construction of a Finite-Field Slide Rule for Undergraduate Students

Marco Abrate
Politecnico di Torino, Italy

ABSTRACT: Math manipulatives and physical math activities offer numerous benefits in the learning process in all educational levels: they provide concrete representations of abstract concepts, thus helping more students to understand them, and they are an opportunity for students to explore and test their understanding of mathematical concepts. Moreover, in active learning activities conducted with tangible objects, students are physically engaged in the lessons, and are given a fun way to practice their math skills, which contributes with retention and positive feeling.
In this article, an active teaching activity aimed at first-year college students is presented, designed to deepen the understanding of finite fields through the construction of a slide rule. The tool presented is easy to make and can be used effectively in a short time. The activity described was carried out as part of a larger workshop on modular arithmetic and the basics of cryptography offered to first-year engineering students at Politecnico di Torino.

Keywords: Mathematics Teaching, Active Learning, Modular Arithmetic, Slide Rule

The Mathematics Enthusiast, **ISSN 1551-3440, vol. 21, no. 1&2**, pp. 88–98

Introduction

Students who are beginning a college career may encounter some difficulties due to some new topics or to the rigor of higher education programs, and often feel unprepared for the academic demand. Without an adequate institutional support, these difficulties may cause a lack of academic achievement that may play a role in the decision to drop out studies [1, 2].
To encourage undergraduate students to continue their studies and to increase their performance in STEM education, some active learning activities can be implemented, so that students become protagonists of the teaching-learning process, responsible for their own educational process, in line with the constructivist paradigm [3, 4, 5, 6, 7]: students can find greater motivation and to have a more confident approach to subjects that prove particularly challenging in the early years of college. Active learning is a broad concept, activating teaching methods and teacher-led learning processes [8, 9, 10]. The use of active learning activities, and in particular laboratories employing the use of concrete objects or implementing engaging learning contexts that foster positive feelings toward particular subjects, is often seen as a solution suitable mainly for primary and middle school students [11]. However, the novelty of some topics and some ways of dealing with concepts already seen makes university students novices in particular contexts, and their vulnerability allows them to be compared to younger students tackling certain topics for the first time [12, 13, 14].
The activity we are proposing concerns an algebra workshop designed for undergraduate Engineering student of the first year, and is part of a larger project involving the activation of several laboratories offered to first- and second-year students at Politecnico di Torino, called La.M.Po. (Laboratorio di Matematica del Politecnico di Torino). Our laboratories aim to integrate active learning into traditional Calculus and Linear Algebra courses [15] and are designed to work with small groups of students, who are involved in the activities through the use of concrete objects and a focus on scientific applications. Our activity covers an introduction to modular calculus, and is part of an preparatory lab on cryptography in which the basics of modular calculus in finite fields and some public-key and private-key cryptographic techniques are presented.
In this paper we will focus our attention on a particular activity in the lab that aims to reflect on the role of prime numbers and finite fields in cryptography and to the construction of some finite fields; since computation within finite fields, especially with regard to the product, is particularly abstract and difficult to accomplish, especially for students who are approaching this type of algebraic structure for the first time, a slide rule, analogous to those introduced for real numbers in the seventeenth century, is constructed in our activity. This tool allows students to quickly perform calculations within finite fields, observing the deep structure underlying these kinds of calculations. Our main objective is to stimulate students to approach the study of algebra, particularly that of finite groups and fields, through the construction of a computational tool capable of implementing the product in multiplicative cyclic groups. Through this tool, students have the opportunity to handle an object that allows them to visualize in a concrete way some concepts that are often perceived as abstract. Moreover, they can increase the level of confidence in algebra through experience, allowing a deeper understanding as well as the development of an appropriate language property. The procedure that we will follow can be a useful teaching tool, usable at any school level if properly adapted to the target audience, to explain the importance of cyclic groups and to motivate the attention that texts place on finding a generator and classifying algebraic structures according to whether or not a single generator can be identified. Furthermore, in the construction the student has the opportunity to try his hand at finding a primitive root of a group, touching on the difficulties encountered in its determination and, at the same time, discovering the great advantages that can result in terms of computational performance. In addition, the realized slide rule makes it possible to perform directly and efficiently some calculations that often discourage students approaching modular arithmetic or the theory of finite fields and their extensions for the first time.

1 Context

Our activity has been proposed to 75 first-year students, divided into three classes of 25 students each. Each class worked for three hours: they participated to an introductory cryptography lab, where they learned the rudiments of modular calculus. Within the laboratory, rest classes modulo n were introduced and modular calculus in finite rings and fields of the type $\mathbb{Z}_n$ was experimented (in special cases where the number of elements was small enough to operate with elementary tools); then the problem of finding the

generators of the multiplicative group of the finite ring was presented, and the possibility of determining a single generator in some special cases, and the advantage of operating with cyclic multiplicative groups was shown. Within this laboratory, thanks to the employment of a slide rule made directly by the students, they were able to acquire a certain manual dexterity in performing calculations even of a certain difficulty in a short time, operating quickly within algebraic structures without the aid of electronic devices, also considering that the most commonly used pocket calculators do not allow modular calculations. Moreover, they can visualize the deeper meaning of the operations they were performing, something made impossible when operating with modular arithmetic by means of a computer.

2 Mathematical background and notations

Here we will see an overview of the principles by which slide rules were invented, how they work, and the algebraic operations (on $\mathbb{R}$) allowed by exploiting the properties of real logarithms (product, inverse calculus, division, calculus of proportions), and we will see how similar principles can be used for implementing analogous operations in cyclic multiplicative groups. For simplicity, we will refer specifically to multiplicative groups of finite field. However, the same procedure that will be described below can be replicated for constructing rulers to operate on any cyclic group.

2.1 The mathematics behind the slide rule

At the turn of the 16th and 17th centuries, the study of the properties of powers and geometric progressions brought out the possibility of performing multiplications by transforming them into sums: these studies led to the introduction of logarithms, defined by John Napier in 1614 and later studied by Napier, Briggs, Gunter, and Oughtred among others. In particular, Gunter, in 1620, was the first to create the slide rule, a tool that allowed various calculations, including multiplication and division, to be performed by exploiting precisely the properties of the newly introduced logarithms. The use of the slide rule, which initially remained limited to a small circle of technicians and scientists, spread widely in the 19th and 20th centuries, until the introduction of faster and more accurate electronic calculators replaced it for good.
The functioning of the slide rule used to perform multiplication and division (and some other derived operations, such as powers, inverse calculation, and others), is based on the possibility of representing any positive real number as an image of a real number through the exponential function (in any a base) and being able to use the groups isomorphism

$$\begin{aligned} a^{\cdot}: \quad (\mathbb{R},+) &\longrightarrow (\mathbb{R}^+,\cdot) \\ x &\longmapsto a^x \end{aligned}$$

to be able to perform the product in $(\mathbb{R}^+,\cdot)$ by means of a sum in $(\mathbb{R},+)$ by exploiting the property whereby

$$a^{x_1+x_2} = a^{x_1} \cdot a^{x_2}.$$

With the slide rule, it is possible to perform, by juxtaposition, the sum between the two numbers x_1 and x_2, interpreted as a^{x_1} and a^{x_2} respectively, so that the sum can be interpreted as the result of $a^{x_1} \cdot a^{x_2}$. The idea that will be developed in the following is to use similar properties of the exponential function in finite fields to make a simple tool to perform products, divisions, powers, inverse calculations, as well as other operations involving the product, in finite cyclic multiplicative groups. In fact, the existence of a primitive root in a cyclic group allows each element of the group to be represented as a power of that element: if we denote by g the generator of the group G, we will have that for all x in G, there exists i in $\mathbb{N}$ such that $x = g^i$; moreover, if $x_1, x_2 \in G$ then there exist i_1 and i_2 such that $x_1 = g^{i_1}$, $x_2 = g^{i_2}$ and, by the properties of exponentials, $x_1 \cdot x_2 = g^{i_1+i_2}$.

2.2 Finite fields

This section is concerned with the mathematical aspects relevant to finite fields and their multiplicative group. All the properties we report are well-known from the elementary theory of cyclic groups and

commutative rings with unity. Let $\mathbb{F}$ be a finite field of characteristic p. $\mathbb{F}$ contains the field R_p of residue classes of the integers $\mod p$

$$R_p = \{1, 2, 3, ..., p-1, p = 0\}.$$

Since the number of elements in $\mathbb{F}$ is finite, the degree $m = (\mathbb{F}/Rp)$ is finite. Let $\omega_1, \omega_2, ..., \omega_m$ be a basis of $\mathbb{F}/Rp$. Then every $f \in \mathbb{F}$ may be uniquely described in the form

$$f = c_1\omega_1 + \cdots + c_m\omega_m$$

where the c_i are elements of R_p for every $1 \leq i \leq m$. The number of elements in $\mathbb{F}$ is therefore $q = p^m$. Hence, the number q of elements in a finite field $\mathbb{F}$ is the $m - th$ power of the characteristic where $m = (\mathbb{F}/Rp)$. Moreover, the $q - 1$ nonzero elements of $\mathbb{F}$ form a multiplicative group of order $q - 1$.

Theorem 2.1. *To each power p^m of a prime p there is exactly one field (apart from isomorphism) with p^m elements.*

Theorem 2.2. *Every finite multiplicative subgroup of a field is cyclic.*

Corollary 2.3. *The multiplicative group of a finite field is cyclic.*

2.2.1 Examples

Let us now give some typical examples of cyclic groups in multiplicative notation. These are examples of groups for which a slide rule can be constructed as described in the following sections.

Example 2.4. *The simplest example of a finite field is that of residue classes of the integers $\mod p$, i.e. the field*

$$\mathbb{F}_p = \{0, 1, \cdots, p-1\}.$$

For example, let us consider the (unique) field of 7 elements

$$\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}.$$

Its multiplicative group $\mathbb{F}_7^*$ is a cyclic group of order 6. It can be seen that the primitive roots of $\mathbb{F}_7^*$ are 3 and 5.

Example 2.5. *Let us construct the field of 3^2 elements. The ground field is $\mathbb{F}_3 = \{0, 1, 2\}$; in $\mathbb{F}_3[x]$, consider the irreducible polynomial $x^2 + 1$. Let ω denote a root of $x^2 + 1$. $\mathbb{F}_3[\omega]$ consists of the elements $a + b\omega$, where $a, b \in \mathbb{F}_3$, and $\omega^2 = 2$. The field $\mathbb{F}_3[\omega]$ has then 9 elements and is sometimes denoted by $GF(9)$ (which stands for Golois field): it is unique (apart from isomorphism), and can be identified with the set of polynomials whose degrees are at most 1, with $x^2 = 2$. Its multiplicative group is cyclic of order $3^2 - 1 = 8$ and the primitive roots are four, namely $x + 2$, $2x + 2$, $2x + 1$, and $x + 1$.*

In the following, we will denote by $\mathbb{F}_q$ the finite field with q elements, where $q = p^m$. It should be noted that the discussion that follows would still be valid for finite rings whose multiplicative group is cyclic; however, in such structures the product between two elements of the multiplicative group would not allow us to represent all the nonzero elements of the ring, so the slide rule construction would only partially describe the ring product.

3 Main activity: making the slide rule for $\mathbb{F}_q^*$

The use of the slide rule is a central part of the proposed workshop, so one of the activities in which students are involved is to build their own paper slide rule, using readily available materials. Although the idea of using slide rules for educational purpose his known [16, 17, 18], the activity proposed in this article is different, both in the type of algebraic structures in which it operates and in the way it is done. In this section we provide a standard procedure to the construction of a multiplicative slide rule in a fixed finite field $\mathbb{F}_q$, where $q = p^m$, p is an odd prime and $m \geq 1$.

The objectives of the activity are:

- to deepen the finite fields structure;

- to discover the properties of cyclic groups through a tangible object to internalize and reinforce the understanding of the same properties through direct experience involving the student's sight and touch;
- learn how to use the slide rule to perform basic operations (multiplication, division, inverse calculation).
- to be more aware of the complexity of calculus and the possibilities of reducing complexities by means of abstractions;
- to enrich the students' culture and stimulate their curiosity about computational tools.

To make the paper slide rule for finite, cyclic groups we use (see Figure 1):

- scissors;
- cardboard;
- paper clip;
- pen or pencil.

Figure 1: Materials to make your own cyclic slide rule.

Once the order q is chosen, it follows that the multiplicative group $\mathbb{F}_q^*$ has $q-1$ elements: thus, we can cut out from the cardboard two regular $(q-1)$-sided polygons (if possible) or two circles[1]. One should be small enough to fit inside the other: for example, we cut out two polygons having circumscribed circumferences of radius 11 cm and 8 cm respectively (or about 4 and 3 inches respectively). Then, make a hole right in the center of the two shapes, place the two templates so that their centers coincide, and fix them using a fastener (Figure 2).

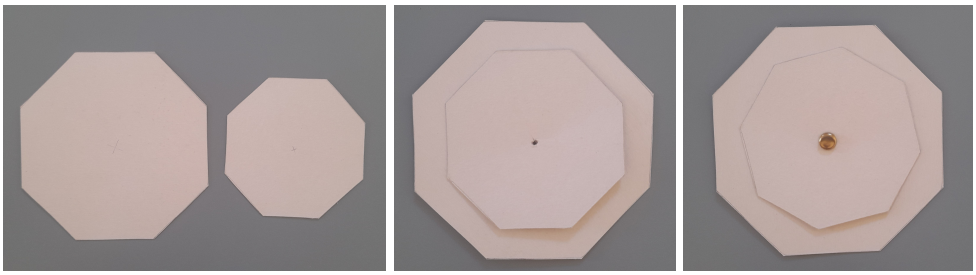


Figure 2: Making your own cyclic slide rule.

[1] As is well known, not all regular polygons are constructible with a ruler and compass, and not all constructible are easy to construct; on the other hand, when the number of sides is large enough, it may not be meaningful to have polygons available, and making something that looks like a circle may be sufficient for our purpose. If a computer, equipped with a software that allows to plot regular polygons having an arbitrary number of sides, and a printer are available, one can still consider having polygons.

Now, we look for a primitive root in the multiplicative group $\mathbb{F}_q^*$, i.e. a $g \in \mathbb{F}_q^*$ whose period is $\phi(q) = q-1$. Hence we can write down a table containing all the powers of the elements in $\mathbb{F}_q^*$ up to the first generator of the group. At this stage, we have a primitive root, and all its powers are listed ordered by exponent: $\mathbb{F}_q^* = \{g, g^2, g^3 \cdots, g^{q-1}\}$. The elements of $\mathbb{F}_q^*$ can be written one on each side of both regular polygons: in particular, we decide to follow the order given by the powers of g and write the numbers clockwise. The multiplicative slide rule for $\mathbb{F}_q^*$ is now ready to be used.
In Figure 3 a slide rule for $\mathbb{F}_7^*$ is shown. It is obtained fixing two regular hexagons: we chose the number 3 as the generator and wrote its ordered powers around the ruler.

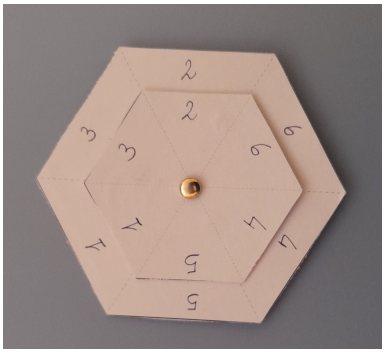


Figure 3: A multiplicative slide rule for $\mathbb{F}_7^*$ obtained with $g = 3$.

A slide rule can also be made to work on a finite field of the type $\mathbb{F}_{p^m}$, where p is a prime and $m > 1$. Let us consider the field $\mathbb{F}_9$, constructed as the set of polynomials whose degrees are at most 1, with operations defined modulo the irreducible polynomial $x^2 + 1$ (see Example 2.5). We choose $g = x + 2$ as a generator of $\mathbb{F}_9^*$, and then we list the powers of g: $\{x + 2, x, 2x + 2, 2, 2x + 1, 2x, x + 1, 1\}$. We realized the slide rule for $\mathbb{F}_9^*$ fixing two octagons and writing the ordered powers of g on their sides (see Figure 4).

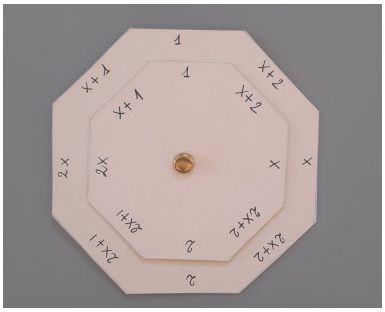


Figure 4: A multiplicative slide rule for $\mathbb{F}_9$, with $g = x + 2$.

3.1 How to use the multiplicative slide rule

The multiplicative slide rule can now be used to perform a number of calculation, such as:

- multiplication;
- inverse calculation;
- division;
- ratios;
- powers.

In the following, we give a brief guide on how to find the results of the listed calculations. We refer to a polygonal slide rule, but the shape of the rule is not meaningful.

3.1.1 Multiplication

The main operation for which the idea of building a slide rule arose is multiplication: from the ability to make products come all the other functions of the instrument. To multiply two numbers, align the side relative to the first number in the inner polygon to the side at 1 of the outer. Find the other number on the same polygon and read across to find the result.
The reason multiplication can be performed this way is to be found in the properties of the powers of generator g and in the way we constructed our tool. In fact, if we start from the initial position where all the numbers are aligned, when we want to calculate $a \cdot b \,(\mathrm{mod}\, p)$ we perform a clockwise rotation of the inner polygon by α steps, where α is such that $a = g^\alpha$ due to order given to the numbers around the slide rule. Now, the number b on the outer polygon can be found β steps away from the 1, moving clockwise, where β is such that $b = g^\beta$. Thus, reading across we find the number corresponding to $g^{\alpha+\beta}$ (i.e. sliding the rule is equivalent to adding the logarithms of a and b $(\mathrm{mod}\, p-1)$), that is we read

$$g^{\alpha+\beta} = g^\alpha \cdot g^\beta = a \cdot b,$$

as expected.
Is straightforward to see that, since the product is commutative, the same result is obtained if one align the side relative to the number a in the outer polygon to the side at 1 of the inner: the result is now on the outer polygon, aligned with the b on the inner. In other words, product commutativity results in the interchangeability of the discs.

Example 3.1. *Suppose we want to evaluate the product* $5 \cdot 4\,(mod 7)$*: we can align the number* 5 *in the inner polygon to the number* 1 *of the outer. Across the number* 4 *on the outer polygon we read* 6*, that is* $5 \cdot 4 \equiv 6\,(mod 7)$ *(see Figure 5a).*
Moreover, moving around the slide rule, we can read the whole list of the multiples of 5 *in* $\mathbb{F}_7$*: in fact, since every element* $c \in \mathbb{F}_7^*$ *is written on the outer polygon, it is aligned with* $5 \cdot c\,(mod 7)$*. That is, we are able to perform* 6 *multiplications at once.*

(a) (b)

Figure 5: The multiplication table of 5 in $\mathbb{F}_7$ and that of x in $\mathbb{F}_9$.

It can be pointed out that, since the roles of the two polygons are interchangeable and being the number 1 *on the inner polygon aligned with the number* 3 *on the outer, we can also read all the results obtained by a multiplication by* 3*; we have thus performed an aggregate of* 11 *multiplications at once (in some configurations of the slide rule some of these operations are possibly repeated).*

Example 3.2. *Let's use the same procedure in* $\mathbb{F}_9$ *as realized in Example 2.5 to evaluate* $x \cdot (2x+1)$ *using the slide rule shown in Figure 4: we can align the* x *in the inner polygon to* 1 *of the outer. Across the polynomial* $2x+1$ *on the outer polygon we read* $x+1$*, that is* $x \cdot (2x+1) \equiv x+1\,(mod(x^2+1))$ *(see Figure 5b).*
Moreover, moving around the slide rule, we can read the whole list of the multiples of x *and the multiples of* $2x+1$ *in* $\mathbb{F}_9$*: here we perform* 15 *multiplications at once.*

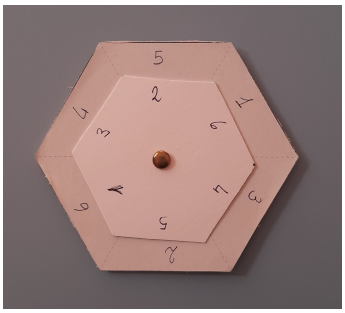
3.1.2 Inverse calculation

Using the slide rule, it is also possible to rapidly find the multiplicative inverse of every element in $\mathbb{F}_q^*$. To find the inverse of an element, align the side relative to the number to invert, say a, of one polygon to

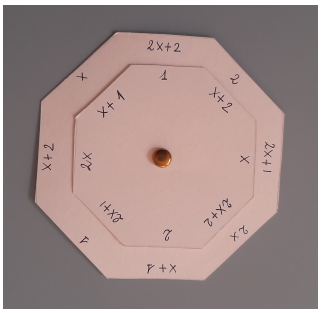
the side at 1 of the other. Find the side at 1 of the first polygon and read across to find the result (call it b).
In fact, it is easy to observe that sliding the rule that way is equivalent to perform the product $a \cdot b$ and find out that the result is 1, that is $b = a^{-1}$. As an example, looking again at Figure 5a, we see that 5 and 3 are the inverse of each other in $\mathbb{F}_7$. Similarly, in Figure 5b it can be seen that in $\mathbb{F}_9$ $2x$ is the inverse of x and vice versa.

3.1.3 Division and ratios

Consider the division $a \cdot b^{-1}$. To perform the calculation, align the two numbers a and b: the result of the division can be read across the number 1 found on the polygon of b. This calculation is indeed a generalization of the inverse calculation, where the number a was assumed to be 1.
Moreover, combining some of the considerations seen above, relating to the interchangeability of the disks or the computation of the inverse, it is easy to observe that, keeping the slide rule in the same position, at 1 on the polygon of a will read the result of $b \cdot a^{-1}$.
In Figure 6, two divisions in $\mathbb{F}_7$ and $\mathbb{F}_9$ are shown. For example, in Figure 6a it can be seen that $4 \cdot 3^{-1} \equiv 6\,(\mathrm{mod}7)$, and in Figure 6b that $x \cdot (x+1)^{-1} \equiv 2x + 2\,(\mathrm{mod}(x^2+1))$.



(a) $4 \cdot 3^{-1} \equiv 6\,(\mathrm{mod}7)$



(b) $x(x+1)^{-1} \equiv 2x + 2\,(\mathrm{mod}(x^2+1))$

Figure 6: Some divisions in $\mathbb{F}_7$ and in $\mathbb{F}_9$.

It is interesting to point out that the same configurations show a number of divisions: in Figure 6a one can see all the pair (a, b) such that $a \cdot b^{-1} \equiv 6\,(\mathrm{mod}7)$, namely $(4, 3)$, $(5, 2)$, $(1, 6)$, $(3, 4)$, and $(2, 5)$; in Figure 6b are shown all the pair (a, b) such that $a \cdot b^{-1} \equiv 2x + 2\,(\mathrm{mod}(x^2+1))$, namely $(2, x+2)$, $(2x+1, x)$, $(2x, 2x+2)$, and so on.

4 Educational considerations

During the workshop held in the classroom, students made slide rules for multiplication in $\mathbb{F}_7$ and $\mathbb{F}_{11}$. Each student designed and constructed his or her own slide rules, taking about 30 minutes: the production of the objects was supervised by the teachers who moderated the discussions among the students involved. Once the slide rules were constructed and their operation was explained, all students were able to easily execute operations within the structures considered. Some very interesting aspects emerged from the classroom observation, which the author suggests as a starting point for further developing the presented activity.

- Giving students the opportunity to critically pose themselves with respect to a definition through discussion and debate is challenging and helps them discover possibilities and implications that they may not always be able to reach on their own, whether due to lack of motivation or merely lack of time.

- This construction of the slide rule usually has a great impact on participants for several reasons. First of all, it is operationally simple enough, but it confronts students with some algebraic aspects that they had not thought much about previously. The search for a primitive root can be very instructive: it can be pointed out that different student can produce different, but in fact equivalent, slide rule depending on the choice of the generator.

These observations can be discussed with the students, in order to highlight some of the abstract properties of finite fields that can have concrete consequences.

- Through this activity, students have the opportunity to handle discrete exponentials, and they can be conducted further to explore the difficulties of dealing with discrete logarithms.
- The manipulation of powers on a slide rule constitute an example of applying the concept of isomorphism between algebraic structures.
- Students can also go beyond the concept of primitive roots and find a level of abstraction whereby one no longer sees the motivation behind a procedure, but handles it at a higher level using a mechanism.
- They also experience positive emotions related to being able to perform the calculations, which are often perceived as complicated and an end in themselves.
- The fact that with the slide rule multiplication, division and ratios are approached in essentially the same way is a consequence of the connection between these operations. This approach allows for nontrivial thinking about these simple operations, and for a broader look at basic arithmetic.
- A step forward can be done in order to introduce powers: a scale of squares can be added on the inner circle, writing below every element of the field the corresponding square (see Figure 7). This update provides a ready-to-use list of squares, which is useful for dealing with quadratic residuals within the field, and allows the introduction of some techniques for calculating possible powers.

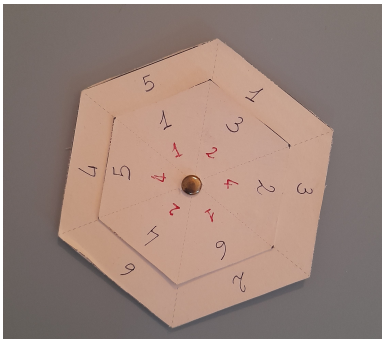


Figure 7: A slide rule for $\mathbb{F}_7$ with the scale of squares.

Looking at the configuration in Figure 7, we can quickly find what is $3^3 \pmod 7$: since $3^3 = 3^2 \cdot 3$, using the squares' scale we read $3^2 \equiv 2 \pmod 7$ and then $3^3 \equiv 2 \cdot 3 \equiv 6 \pmod 7$.

- There are many cases where introductory cryptography workshops are offered to young students [19, 20, 21]. The activity proposed in this article can be adapted for high school or middle school students, reducing the formalism but maintaining the content: it can provide a tool for teachers and students to make the learning process activated in the lab more effective.

5 Conclusion and Remark

Active learning activities and experiential-based learning can also be designed and conducted successfully at the college level. The use of manipulatives in learning mathematical concepts offers students a different way of learning and engaging in the lesson, and allows them to consolidate learning in a positive context. The laboratory activity presented aims to engage undergraduate students in learning in the area of finite fields. The opportunity for students to handle a tool whose behavior is based on the seemingly abstract properties of these structures allows them to give concrete form to a new topic and approach it in an engaging way that increases interest and motivation.
The main part of this paper is centered on the description of the activity of constructing a slide rule to perform multiplications in a finite field and the teaching aspects of this activity. The students who performed this activity showed interest in the subject; they also felt positive and successful in better

understanding the concepts with the support of the manipulatives and because of the possibility of easily performing operations that are challenging to perform in their heads.

References

[1] Meyer, M., & Marx, S. (2014). Engineering Dropouts: A Qualitative Examination of Why Undergraduates Leave Engineering. *Journal of Engineering Education*, 103, 525–548.

[2] Casanova, J. R., Vasconcelos, R., Bernardo, A. B., & Almeida, L. S. (2021). University Dropout in Engineering: Motives and Student Trajectories. *Psicothema*, 33(4), 595–601.

[3] Gavalcová, T. (2008). On Strategies Contributing to Active Learning. *Teaching Mathematics and its Applications*, 27(3), 116–122.

[4] Sofroniou, A., & Poutos, K. (2016). Investigating the Effectiveness of Group Work in Mathematics. *Education Sciences*, 6, 30–45.

[5] Holley, E. A. (2017). Engaging engineering students in geoscience through case studies and active learning. *Journal of Geoscience Education*, 65, 240–249.

[6] Christie, M., & de Graaff, E. (2017). The philosophical and pedagogical underpinnings of active learning in engineering education. *European Journal of Engineering Education*, 42(1), 5–16.

[7] Freeman, S.; Eddy, S. L., McDonough, M., Smith, M. K., Okoroafor, N., Jordt, H., & Wenderoth, M. P. (2014). Active learning increases student performance in science, engineering, and mathematics. *Proceedings of the National Academy of Sciences*, 111, 8410–8415.

[8] Felder, R. M., & Brent, R (2009). Active learning: An introduction. *ASQ Higher Education Brief*, 2, 4–9.

[9] Prince, M. J., & Felder, R. M. (2006). Inductive teaching and learning methods: Definitions, comparisons, and research bases. *Journal of Engineering Education*, 95, 123–138.

[10] Webb, N. M., Troper, J. D., & Fall, R. (1995). Constructive activity and learning in collaborative small groups. *Journal of Educational Psychology*, 87, 406–423.

[11] Sarama, J., & Clements, D. H. (2016). Physical and Virtual Manipulatives: What Is "Concrete"?. In Moyer-Packenham, P. (eds), *International Perspectives on Teaching and Learning Mathematics with Virtual Manipulatives*. Mathematics Education in the Digital Era, vol 7. Springer, Cham.

[12] Miller, D. A., & Schraeder, M. (2022). Using worked examples with active learning in a large lecture college algebra course. *International Journal of Education in Mathematics, Science, and Technology (IJEMST)*, 10(1), 1–23.

[13] Monte, J. (2021). An Exploration of Manipulatives in Math Education, *Undergraduate Review*, 16, 200–213.

[14] Moore, D. (2001). Using Manipulatives in Undergraduate Mathematics Courses. *Journal of Mathematics and Science: Collaborative Explorations*, 4(2), Article 10.

[15] Ceragioli, F., & Spreafico M. L. (2020). Tangible Tools in Mathematics for Engineering Students: Experimental Activity at Politecnico di Torino. *Digital Experiences in Mathematics Education* 6, 244–256.

[16] Wolbert, W. J. (2012). Sliding through Logarithms. *The Mathematics Teacher*, 106(4), 320.

[17] Sowell, K. O., & Mcguffey J. P. (1971). Nondecimal Slide Rules and Their Use in Modular Arithmetic, *The Mathematics Teacher*, 64(5), 467–472.

[18] Johnson, D. A. (1954). A Slide Rule for Addition and Subtraction of Numbers Having the Base 12, *The Mathematics Teacher*, 47(5), 339.

[19] Long-Yuan, Y. (2007). Teaching Cryptography Activity in Taiwan's High Schools, *Proceedings of the 2007 conference on Supporting Learning Flow through Integrative Technologies*, IOS Press, NLD, 553–560.

[20] Lodi, M., Sbaraglia, M., & Martini, S. (2021). Big Ideas of Cryptography in K-12. `https://bigideascryptok12.bitbucket.io/`

[21] Bell, T., Thimbleby, H., Fellows, M., Witten, I., Koblitz, N., & Powell, M. (2003). Explaining cryptographic systems, *Computers & Education*, 40(3), 199–215.

DISMA, Politecnico di Torino, Turin 10129, Italy
Email address: `marco_abrate@polito.it`