The Mathematics Behind Cryptocurrencies and Blockchain

Elena Soledad Jiménez-Ayala
elena.jimenez@upct.es
Departmento de Matemáticas y Estadística
Universidad Politécnica de Cartagena
Calle Dr. Fleming S/N - 30203 Cartagena
Spain

Juan Medina
juan.medina@upct.es
Departmento de Matemáticas y Estadística
Universidad Politécnica de Cartagena
Calle Dr. Fleming S/N - 30202 Cartagena
Spain

Abstract

In day-to-day education, when we introduce a new mathematical concept in class, students often ask: what is its purpose? It is then useful and enriching to be able to present some interesting current technology to which the mathematics can be applied. We show some of the mathematics that underlies cryptocurrencies, specifically bitcoin and the technology behind it, known as the blockchain. Many people talk about the blockchain as being one of the most important innovations of recent times, since it can be applied in a wide variety of fields, from economy to education. A vital aspect of the mathematics present in cryptocurrencies and the blockchain is cryptography, mainly in connection with elliptic curves. Having some knowledge of cryptography, therefore, may be appropriate for economists, engineers, scientists in general, and mathematicians. However, the way to present it to each of these groups should be different. We examine the approach and the contents by which this topic should be introduced in class, and distinguish to whom the training is aimed.

1 Introduction

Sometimes it is wanted to differentiate between those aspects of mathematics that have been applied to other fields of knowledge or related to real life, and those that have been used only in their own development. For many years, it was thought that topics in number theory, such as divisibility or prime numbers, were examples of these latter mathematics. However, over the past few decades, thanks to the development of computing and the Internet, it has become important to be able to transmit messages or perform online procedures and, at the same time, make it impossible for them to be intercepted and become known by someone unwanted . Cryptographic tools are essential for this purpose and number theory has always been a part of mathematics vital for the development of cryptography. By contrast, cryptocurrencies have appeared only in very recent years, the most important of them being the bitcoin. This cryptocurrency incorporates an associated technology called the blockchain, whose usefulness surpasses its application to bitcoin, Its wide utility is the reason that the blockchain is considered to be one of the most important discoveries of the past few years. The blockchain consists of databases linked to one another in such a way that they are unalterable. From the entries of these databases, which can be represented as matrices, to the security, which is guaranteed by the use of cryptographic tools, mathematics is the key to blockchain success. Since the blockchain has numerous applications, in technological fields and even in social sciences, as well as economics, a basic knowledge of mathematical tools could prove very useful for many professionals. On the other hand, we could use the importance of the blockchain as a reason to give our students a complementary trainning in some mathematical concepts. Despite the fact that these contents are not normally studied in secondary education or university, students are fully capable of understanding them. The training will depend on to whom it is addressed. Students of mathematics and computer science may already be familiar with some of these concepts, whereas for others, it will be necessary to give only an informal type training, with the simple objective of knowing a little behind this technology. In what follows, we will describe the contents that could be included when giving training to students and indicate the suitability of these according to the type of students to whom the training is addressed.

2 A brief historical introduction to bitcoin and blockchain

The origin of bitcoin is a document [1] published in 2009 in a cryptography forum by a programmer known by the pseudonym of Sathosi Nakamoto. The objective was to create a virtual currency, without the need for intermediaries when carrying out transactions yet, at the same time, enabling complete confidence in the system. To achieve this, the bitcoin is accompanied by a free technology, the blockchain, which consists of a computer protocol similar to a database that is decentralised, that is, all the information is collected using different computer equipment of users throughout the world. An advantage of the blockchain is that its usefulness goes far beyond bitcoin, since it can be used in other currencies and even in other sectors, including business, education, and health.

The value of the bitcoin is determined by supply and demand. At first, the value of was close to 0; consequently, this currency was of interest only to small groups of people close to the world of computing. However, at the beginning of December 2017 the bitcoin reached a value of more than US$10000, attaining its highest point on the 17th of that month, with a value near $20000. As a result, many of the initial buyers made a huge profit, which encouraged others to invest in this currency. However, a few days later the price of bitcoin fell by almost 20%, reaching a value close to $3,500$ at the beginning of 2019. Such wide fluctuations are why some economic experts have described bitcoin as a simple speculative instrument. In recent times, bitcoin has climbed in value again, exceeding $10,000$. In June 2019, Facebook announced the creation of its own cryptocurrency, called Libra. Some experts thought this might be the end of bitcoin, but, on the contrary, its value rose following the announcement.

One of the strengths of the blockchain is the inviolability of its records, and the main reason for this is the mathematics and cryptography behind it. Each new blockchain entry is linked to the previous one, in a process known as sealing, so that the identity of the user who made it is kept anonymous and no entry can be deleted or modified. Hundreds of computers compete, carrying outing numerous complex operations, and the first to complete the process receives a commission. At that moment, the other computers must check that all the calculations have been made correctly. This whole process is known as mining.

Anyone can buy bitcoins. In order to do this, you must install an electronic wallet on your mobile or computer device, in which your bitcoins will be deposited. At any given instant, the user has a bitcoin address, which allows them to carry out operations; a new bitcoin address is generated for each new operation. These bitcoin addresses are used in the sealing process.

3 Introduction to modular arithmetic

When working with the cryptography of elliptical curves we operate within a finite field. Thus we consider it necessary that our students have a basic understanding of modular arithmetic and finite fields. However, to achieve merely an informal level of knowledge we could omit these contents and work directly with elliptic curves on $\mathbb{R}$.

Students of mathematics and computer science are accostumed to working with such algebraic structures. On the other hand, students of engineering, science, and economics are unlikely to have the requisite knowledge and so must be introduced to it. In addition, we know from experience that for many students it is not easy to understand modular arithmetic, in which seemingly strange situations can arise such as $1 + 1$ equals 0. Furthermore, understanding the concepts of equivalence relations and quotient set is not simple. Therefore, we think it is necessary to complete the introduction of all these concepts with numerous examples and exercises. The first step should be to introduce equivalence relations. We truly believe that the best way to do this is by reviewing some examples that the students have already studied, even though they may have studied them in a different context.

The first time a student encounters a binary equivalence relation is when they study equivalent fractions. As we know, there are sets of equivalent fractions, and the object is to choose one that represents them all, namely the simplest one, taking into account that if it is negative, the minus appears above.

A second example of an equivalence relation that students will have studied is the relationship of vectors in the plane: two non-zero, fixed vectors are equivalent if they have the same magnitude and direction. As in the case of fractions, from each set of vectors we choose a representative one, which, as we know, is the equivalent vector that originates from the origin of coordinates $(0, 0)$. This is how the concept of a free vector arises: we can represent a free vector by a point, which is the end of the corresponding representative.

The first objective of these examples is to enable the student see that in both models the path followed is the same: we establish a two-to-two relationship between the elements of the set, we group the elements that are related, and we choose a representative of each group. Now we are able to introduce the concepts of equivalence relation, quotient set, and representatives, since our students can see them as something familiar since they will have in mind examples

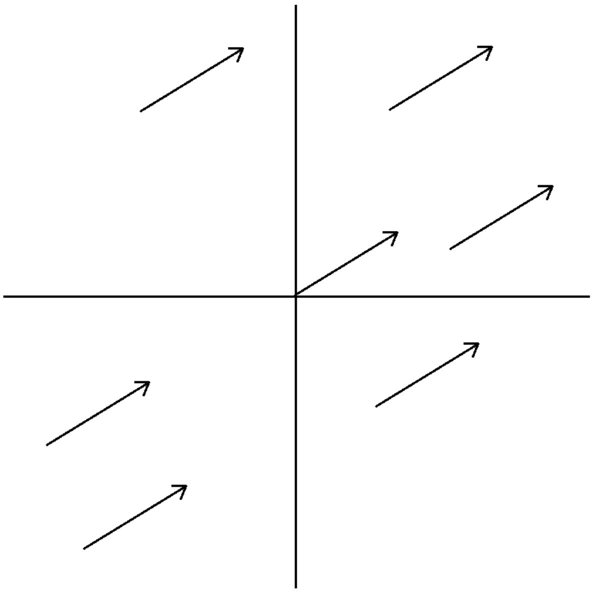

Figure 1: Equivalent fixed vectors and representative

that they know well.

Next we can introduce the modular arithmetic. To do this we usually choose an example based on the days of the week. First, we assign a number to each day of the week, starting from 0, which corresponds to Sunday, up to 6, which corresponds to Saturday.

Sunday	0
Monday	1
Tuesday	2
Wednesday	3
Thusday	4
Friday	5
Saturday	6

Let us consider, for example, Wednesday, which corresponds to the number 3. Adding any multiple of 7, that is, $3 + 7n$, where n is an integer, means that we have moved forward an integer number of weeks and ended up back on the same day.

Thus, we can identify all the numbers that have the form $3 + 7n$, i.e. 3, 10, 17, 24, ..., with Wednesday. A similar process can be applied to the other days of the week. As we are working with the 7 days of the week, it is said that we are working with the integers modulo 7.

We can define a binary equivalence relation in the set of integers: two integers a and b are related if and only if they represent the same day of the week. That is:

$$a \cong b \text{ mod.7 if } a - b \text{ is a multiple of 7.}$$

For this binary equivalence relation, we can establish a quotient set whose elements coincide with the days of the week, or, numerically we can assign them numbers, adding a bar above:

$$\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},\ \bar{4},\ \bar{5},\ \bar{6}.$$

We can denote this quotient set by $\mathbb{Z}_7$ (set of integers modulo 7).

In this set we can define the operations sum and product, based on the ordinary sum and product but reducing the results modulo 7. Our set along with these operations has the structure of field.

Once we have worked with this particular example for $n = 7$, we can generalise the process to any positive integer. So, if n is a positive integer, we define the binary equivalence relation:

$$a \cong b \text{ mod.} n \text{ if } a - b \text{ is a multiple of } n.$$

and we denote by $\mathbb{Z}_n$ the quotient set. As in the previous example we would have:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}.$$

In this set we can also define the operations sum and product modulo n. However, in order to ensure that every non-zero element has an inverse, n must be a prime number. We denote by $\mathbf{F}_q$ the finite field of q elements.

Now we are able to work with particular examples, both the operations sum and product, as long as the calculation of opposites and inverses involves invertible elements. Being able to obtain the invertible elements for n small, testing with the different elements, or doing so using the identity of Bezout, which says that if a, b are integers with $\gcd(a, b) = d$, then there are integers r, s such that:

$$a \cdot r + b \cdot s = d.$$

So, if we want to calculate the inverse of $\bar{a}$, $0 \leq a \leq p - 1$ in $\mathbb{Z}_p$, where p a prime number (then $\gcd(a, p) = 1$), there exist integers r, s such that $a \cdot r + p \cdot s = 1$, from which it is clear that $\bar{a}^{-1} = \bar{r}$. To obtain r and s in the previous expression, we can use the Euclidean algorithm. The Maxima software also incorporates the command gcdex(), in which when we write , gcdex(a, p) we obtain the triple $(r, s, \gcd(a, p)) = (r, s, 1)$.

Here, it would also be possible to introduce finite fields of p^n elements, where p is a prime number and $n > 1$, but we believe that this process could be very complicated except for mathematics and computer students.

4 Review of some cryptographic algorithms

Since our goal is to describe the cryptographic tools involved in bitcoin and blockchain, we think it would be interesting to provide a short introduction to cryptography and present some examples of the ideas behind some cryptographic algorithms.

Cryptography is a discipline whose objective is to encrypt messages so that they cannot be deciphered except by the intended recipient.

One of the oldest cryptographic algorithms involves simple manipulation of the 26 letters of the alphabet:

$$\{A, B, \ldots, Z\}$$

To encrypt a message we change each letter to the one obtained when we move N positions to the right. (When we reach the end, we continue counting from the beginning.) In this case, the key would be N, since this value allows us to encrypt and decrypt messages. A person who knew the key would be able to get the initial message just by swapping each letter for the one obtained by moving N positions to the left.

However, this cryptographic algorithm is very easy to decipher. All that has to be done is to try all the possible values of N (in this case there are 26 possible ones) until we get a message that makes sense.

There are some generalisations of the previous procedure, in which, instead of operating letter by letter we deal with blocks of n letters, working now with vectors and matrices.

The above methods correspond to what are known as symmetric cryptographic algorithms. In these, we work with a single key which is known to the individuals involved in the communication. This key, allowing the sender and the recepient to encrypt and decrypt messages, must remain inaccessible to outsiders. Consequently, one of the main problems that stems from this kind of system is the distribution of the keys among the participants of the communication.

There are also other types of algorithms called asymmetric or public key. In these, each of the participants in an encrypted communication has a public key, which is accessible to everyone, and a private key, which is known only to the owner. These keys are related to each other, and the use of them allows us to encrypt and decrypt messages. If user A sends a message to another user B, A will use B's public key so that only B can decrypt the message (by using their private key). Sometimes, both types of encryption are used for a communication: an asymmetric algorithm for communication and a symmetric algorithm for keys exchange.

Symmetric algorithms are based on mathematical processes that are simple in one sense but computationally unfeasible in another.

One of the best known cryptographic algorithms, RSA (which was created in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman), is based on the fact that given two prime numbers, p and q, of a certain size, the calculation of the product of these numbers is quite easy, $n = p \cdot q$. However, if we know the product n, despite the fact that our prime numbers satisfy certain properties, it is not feasible to obtain p and q from it.

Another very important cryptographic algorithm is the Diffie-Hellman algorithm, created by Whitfield Diffie and Martin Hellman. It consists of a protocol for the generation of common keys between two individuals. As in the case of RSA, this algorithm is based on a mathematical problem that is simple in one sense and enormously complicated in the other. The same is also true of problems that involve the discrete logarithm.

The concept of the discrete logarithm is analogous to that of the traditional logarithm but involves a finite field F_q. Assuming that $a, b\, in \mathbf{F}_q$ where b is a power of a, the logarithm in base a of b is defined as follows:

$$\log_a b = n \mid a^n = b$$

So, given a and n, the calculation of $b = a^n$ is very simple. However, if we start from b, which is a power of a, and take into account that we are working in a field $\mathbf{F}_q$ with q large, it is usually very difficult to calculate the result of the discrete logarithm n.

Later we will talk about the cryptographic algorithm used in the bitcoin and the blockchain, but we note here that the basis of it involves the discrete logarithm of an elliptic curve.

5 Introducing elliptic curves

In this section we are going to work with elliptic curves on $\mathbb{R}$. Let us consider a cubic polynomial $x^3 + ax + b$ without multiple roots. An elliptic curve is the set of points (x, y) satisfying the equation:

$$y^2 = x^3 + ax + b,$$

along with a point O called the point at infinity.

In order to obtain points on an elliptic curve, we only have to give real values to the unknown x, substitute in the right side of the previous expression, and see if the result is a square in $\mathbb{R}$, that is, a real number greater or equal to 0.

As we have mentioned before, in bitcoin and blockchain we are going to work with elliptic curves, specifically with the curve:

$$y^2 = x^3 + 7,$$

the graphic representation of which is:

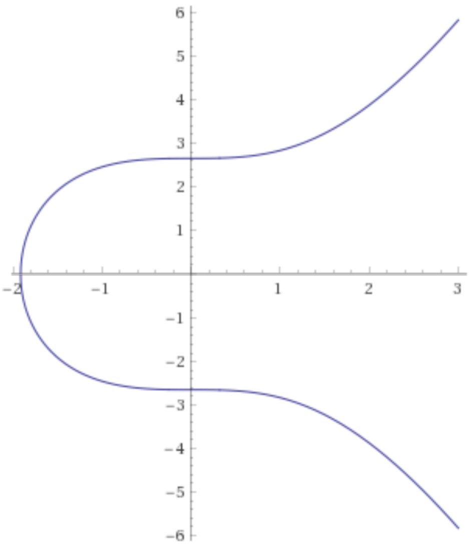

Figure 2: Graph of an elliptic curve

In an elliptic curve we can define a sum operation. The point O will be the neutral element of the sum, that is, $P + O = O + P = P$ for every point P of the curve.

Now, if we consider two different points, P and Q, on the curve, then the sum of them is obtained as follows:

1. We draw the straight line r that passes through the points P and Q.

2. This line r cuts the curve at another point, then the sum $P + Q$ is the symmetric point of this new point with respect to the $x - axis$.

In the following image we can see an example that shows how to obtain the sum of two points P and Q from the previous curve.

Finally, let us explain how to calculate the sum of a point P with itself, that is $2P$.

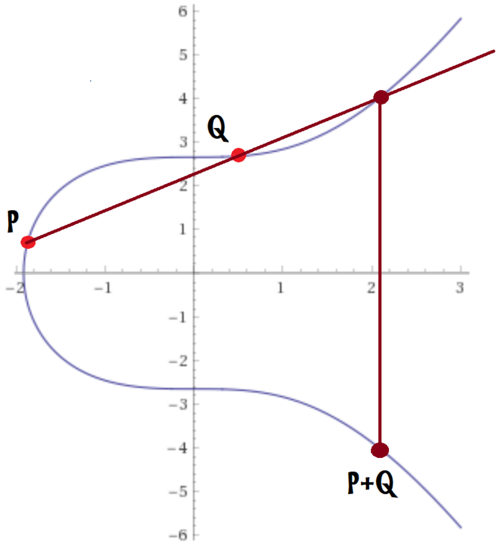

Figure 3: Sum of different points in an elliptic curve

1. We draw the straight line r which is the tangent line to the curve at the point P.
2. This line r cuts the curve at another point. Then $2P$ is the symmetric point of this point with respect to the $x - axis$.

In the following picture we can see an example that shows how to calculate the double of a point P from the previous curve.

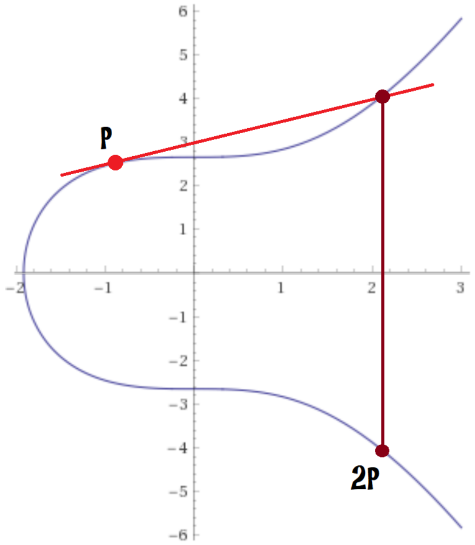

Figure 4: Twice a point in an elliptic curve

Following this process, we have that the set of points of an elliptic curve with this sum operation satisfies the associative property, the existence of the neutral element, which is O, and the existence of a symmetric element for every point on the curve. Thus, we have an abelian group.

It is not difficult to obtain analytical expressions for the calculation of the sum and the double of a point on an elliptical curve. Let us consider two points of an elliptic curve $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. The sum is calculated as follows:

$P + Q = (x_3, y_3)$ where:

$$x_3 \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2,$$

$$y_3 = -y_1 + (\left(\frac{y_2 - y_1}{x_2 - x_1} \right) \cdot (x_1 - x_3)$$

And for the double P, we have $2P = (x_3, y_3)$ where:

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1} \right) - 2x_1,$$

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1} \right) \cdot (x_1 - x_3).$$

We will now generalise the concept of an elliptic curve for the case of a finite field $\mathbf{F}_q$. For simplicity, we will work with elliptic curves on characteristic fields other than 2 and 3 and, as we have done before, the elliptic curves are the points (x, y) that satisfy an equation with the form:

$$y^2 = x^3 + ax + b,$$

also verifying that the polynomial $x^3 + ax + b$ does not have multiple roots, along with the infinity point O.

In this case, we can define the operations sum and product by a number from the previous expressions. Thus, the set of points of an elliptic curve with the sum operation also has abelian group structure.

6 Cryptographic elements in bitcoin and blockchain

The cryptographic algorithm used in the bitcoin and the blockchain is based on the discrete logarithm for elliptic curves on finite fields, which is similar to the discrete logarithm in a finite field. Thus, if we consider an elliptic curve c on a finite field $\mathbf{F}_p$, then the problem of the discrete logarithm consists of, given two points $P, Q \in c$, finding, if there exists a $n \in \mathbb{Z}^+$ such that $nP = Q$.

With the discrete logarithm on elliptic curves we get a new mathematical problem that is simple in one direction but very complicated in the other. As a result, given $n \in \mathbb{Z}^+$ and $P \in c$, the computation of $Q = nP$ is computationally tractable. On the other hand, given P and Q, obtaining the discrete logarithm, that is, n, is a very difficult problem when n is large.

The complexity of the sum operation on an elliptical curve indicates that the discrete logarithm of an elliptic curve is much more intractable than the corresponding one for finite fields.

As a result, the use of algorithms in elliptic curves allows us to work with shorter keys while still achieving a high level of security.

A question to consider is how to calculate nP with n large in an efficient way. One way to do this would be n times P; however, this procedure is not at all adequate. The most suitable way to calculate nP is by using the method of successive squares.

At first, this method is used to calculate powers efficiently (hence the successive squares), but it can also be used for the calculation of nP. Let us show how we do it.

First of all, we obtain: $P, 2P, 4P, \ldots, 2^r P$, where $2^r \leq n \leq 2^{r+1}$, noting that each of the elements above is double the previous one.

Then, we calculate the binary expression for n:

$$n = \sum_{i=0}^{r} a_i 2^i,$$

where, substituting the values obtained previously and making these sums, we obtain:

$$nP = a_0 P + a_1(2P) + \ldots + a_r(2^r P),$$

For instance, if we want to calculate $13P$, as $13 = 2^3 + 2^2 + 2^0$, we have to calculate P, $2P$, $4P$, $8P$, so:

$$13P = 8P + 4P + P$$

As we have said before, for the bitcoin and the blockchain the elliptic curve is:

$$y^2 = x^3 + 7,$$

over the field $\mathbf{F}_p$ where:

$$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951.$$

7 Informative videos about mathematics of bitcoin and blockchain

In collaboration with David Darling, we have created some informative videos that are published on the YouTube video portal at the following links:

Modular arithmetic: `https://www.youtube.com/watch?v=4oAa0v7aYGs` The maths behind bitcoin: `https://www.youtube.com/watch?v=UMb0X8qUpBI`

8 Acknowledgements

The authors would like to thank David Darling for his help and his collaboration in recording the videos.

References

[1] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, Publicly available at the URL `https://bitcoin.org/bitcoin.pdf`, 2009.

[2] Koblitz, N., *A course in Number Theory and Criptography*, Springer Verlag, New York, 1987.

[3] [3] Silverman, J. H., *). A Friendly introduction to number theory*, Prentice-Hall, New jersey, 1997.

[4] Silverman, J. H., Tate, J. T., *Rational Point son Elliptic Curves*, Springer, 1994.

[5] Shemanske, T. R., *Modern Cryptography and Elliptic Curves*, American Mathematical Society 2017.