Mathematics in Bitcoin

Beulah Evanjalin

July 2024

Bitcoin relies heavily on mathematics to operate securely and efficiently. At its core, Bitcoin is a complex system with various mathematical principles to ensure the integrity and security of transactions. Understanding these principles is critical for anyone who wants to effectively contribute to the Bitcoin ecosystem.

Cryptography is fundamental to Bitcoin's existence. This ensures that transactions are secure and that the blockchain remains tamper-proof. Probability and statistics are essential for understanding the randomness and predictability of Bitcoin mining. Algorithms and data structures are the backbone for efficient transaction processing and block formation. Graph theory helps us understand the network of nodes that verify and propagate transactions across the Bitcoin network. Additionally, Boolean algebra, linear algebra, and calculus contribute to the development and improvement of various Bitcoin functions.

1 Divisors and Factors

1.1 Divisor

An integer n is a divisor of another integer i if i can be written as $i = qn$ for some integer q. This means that when you divide i by n, you get another integer q with no remainder.

Key points:

- A divisor n of i must divide i without leaving a remainder.
- The result of dividing i by n must be an integer.
- If n is a divisor of i, then i can be written as $i = qn$, where q is an integer.

Example:

3 is a divisor of 12 because $12 = 4 \times 3$.

1.2 Trivial Divisors

For any integer i, the divisors 1 and i itself are called trivial divisors. These are the simplest divisors that any non-zero integer has.

Example:

The number 12 has 1 and 12 as its trivial divisors.

1.3 Factors

A factor of an integer i is a positive integer that is a nontrivial divisor of i. This means a factor is a positive divisor of i other than 1 or i itself.

Example:

2 and 6 are factors of 12, but 1 and 12 are not considered factors in this context because they are trivial divisors.

1.4 Prime Integer

A prime integer is a positive integer greater than 1 that has no nontrivial divisors other than itself. In other words, a prime number has exactly two distinct positive divisors: 1 and itself.

Example:

5 is a prime number because its only positive divisors are 1 and 5.

2 Modular Arithmetic

Modular arithmetic is a system of arithmetic for integers, where numbers wrap around after reaching a certain value, known as the modulus.

2.1 Euclidean Division Algorithm

Given a positive integer n, any integer i can be uniquely expressed as:

$$i = qn + r$$

where q is the quotient (an integer) and r is the remainder, and it lies in the range $0 \leq r < n$.

This representation is based on the Euclidean division algorithm, which repeatedly subtracts n from i until the remainder r is within the desired range.

2.2 Modulo Operation

The remainder r when i is divided by n is denoted as $i \mod n$. The set of all possible remainders when dividing by n is:

$$R_n = \{0, 1, 2, \ldots, n - 1\}$$

An integer i is divisible by n if and only if $i \mod n = 0$.

2.3 Modular Arithmetic

Modular arithmetic involves performing arithmetic operations (addition, subtraction, multiplication) on the elements of the remainder set R_n. The rules for modular arithmetic are derived from the rules for integer arithmetic.

Example

Consider the modulus $n = 5$. The possible remainders when dividing by 5 are:

$$R_5 = \{0, 1, 2, 3, 4\}$$

Here are a few examples of how numbers wrap around in modular arithmetic:

- $7 \mod 5 = 2$ because when 7 is divided by 5, the remainder is 2.
- $12 \mod 5 = 2$ because when 12 is divided by 5, the remainder is 2.
- $19 \mod 5 = 4$ because when 19 is divided by 5, the remainder is 4.
- $-3 \mod 5 = 2$ because when -3 is divided by 5, the remainder is 2 (we add 5 to -3 to get a positive remainder: -3 + 5 = 2).

For negative integers, we adjust by adding the modulus until we get a non-negative remainder.

2.4 Addition and Multiplication in Modular Arithmetic

Let $r = i \mod n$ and $s = j \mod n$. Then, as integers, r and s can be written as:

$$r = i - qn$$

$$s = j - tn$$

for some integers q and t.

The modular arithmetic operations are defined as follows:

Addition

When adding two integers modulo n:

$$(r + s) \mod n = (i + j) \mod n$$

This is because:

$$r + s = (i - qn) + (j - tn) = i + j - (q + t)n$$

Hence:

$$(r + s) \mod n = (i + j) \mod n$$

Multiplication

When multiplying two integers modulo n:

$$(rs) \mod n = (ij) \mod n$$

This is because:

$$rs = (i - qn)(j - tn) = ij - qjn - itn + qtn^2$$

Since qtn^2 is a multiple of n, we have:

$$rs \mod n = ij \mod n$$

The modular addition and multiplication operations can be summarized as:

$$r \oplus s = (r + s) \mod n$$

$$r \otimes s = (rs) \mod n$$

where r and s are elements of the remainder set R_n.

2.5 Greatest Common Divisor (GCD)

An important concept related to modular arithmetic is the greatest common divisor. The gcd is particularly useful in solving congruences and understanding the properties of numbers in modular arithmetic.

The greatest common divisor (gcd) of two integers a and b is the largest positive integer d such that $d \mid a$ and $d \mid b$. In mathematical notation, we write:

$$\gcd(a, b) = d$$

where $d \mid a$ means that d divides a and $d \mid b$ means that d divides b.

Example

Consider the integers $a = 56$ and $b = 98$.
Divisors of $56 : \{1, 2, 4, 7, 8, 14, 28, 56\}$
Divisors of $98 : \{1, 2, 7, 14, 49, 98\}$
The common divisors are $\{1, 2, 7, 14\}$, and the greatest common divisor is 14.

Therefore,

$$\gcd(56, 98) = 14$$

Modular arithmetic plays a crucial role in Bitcoin, particularly in the field of cryptography that secures the network.

Example:

Bitcoin uses a specific type of public-key cryptography called Elliptic Curve Digital Signature Algorithm (ECDSA). ECC relies heavily on modular arithmetic, particularly for operations on the secp256k1 curve, which is defined by the equation:

$$y^2 = x^3 + 7 \mod p$$

where p is a large prime number. Points on this elliptic curve are used to generate public and private keys, with all operations (addition and multiplication) performed modulo p.

3 Groups

A group is a set of elements $G = \{a, b, c, \ldots\}$ and an operation $\oplus$ that satisfies the following axioms:

1. **Closure**: For any $a \in G$ and $b \in G$, the element $a \oplus b$ is in G.
2. **Associative Law**: For any $a, b, c \in G$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. **Identity**: There is an identity element 0 in G such that $a \oplus 0 = 0 \oplus a = a$ for all $a \in G$.
4. **Inverse**: For each $a \in G$, there is an inverse $-a$ such that $a \oplus (-a) = 0$.

In general, it is not necessary that $a \oplus b = b \oplus a$. A group G for which $a \oplus b = b \oplus a$ for all $a, b \in G$ is called **abelian** or **commutative**.

4 Finite Cyclic Groups

A finite cyclic group is a finite group G with a particular element g in G, called the **generator**, such that each element of G can be expressed as the sum $g \oplus g \oplus \ldots \oplus g$ (repeating g some number of times). Thus, each element of G appears in the sequence of elements $\{g, g \oplus g, g \oplus g \oplus g, \ldots\}$. We denote such an i-fold sum by ig, where i is a positive integer and g is a group element.
i.e.,

- $1g = g$
- $2g = g \oplus g$
- $ig = g \oplus \ldots \oplus g$ (with i terms)

Since g generates G and G includes the identity element 0, we must have $ig = 0$ for some positive integer i. Let n be the smallest such integer; thus $ng = 0$ and $ig \neq 0$ for $1 \leq i \leq n - 1$. Adding the sum of j gs for any $j > 0$ to each side of $ig \neq 0$ results in $(i + j)g \neq jg$. Thus the elements $\{1g, 2g, \ldots, ng = 0\}$ must all be different.

Example: Cyclic Group of Order 4

Consider a cyclic group G of order 4, which means it has 4 elements. Let the generator be g. The elements of G can be written as:

$$G = \{0, g, 2g, 3g\}$$

where 0 is the identity element and $ng = 0$ for $n = 4$. The addition table for this group is:

$\oplus$	0	g	$2g$	$3g$
0	0	g	$2g$	$3g$
g	g	$2g$	$3g$	0
$2g$	$2g$	$3g$	0	g
$3g$	$3g$	0	g	$2g$

Here, each element is generated by repeated addition of g.

Example: Cyclic Group of Integers Modulo 5

Consider the group of integers modulo 5 under addition, denoted $\mathbb{Z}_5$. The generator can be 1, and the group elements are:

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

The addition table for this group is:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

In this group, each element is generated by repeated addition of 1:

- $1 \cdot 1 = 1$
- $2 \cdot 1 = 1 + 1 = 2$
- $3 \cdot 1 = 1 + 1 + 1 = 3$
- $4 \cdot 1 = 1 + 1 + 1 + 1 = 4$
- $5 \cdot 1 = 0$ (since $5 \equiv 0 \pmod 5$)

This shows that $\mathbb{Z}_5$ is a cyclic group with generator 1.

5 Fields

A field is a set F of at least two elements, with two operations $\oplus$ (addition) and $*$ (multiplication), for which the following axioms are satisfied:

1. **Abelian Group under Addition**: The set F forms an abelian group under the operation $\oplus$. This means:
   - **Closure**: For any a, b in F, the result $a \oplus b$ is also in F.
   - **Associativity**: For any a, b, c in F, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
   - **Identity Element**: There exists an element 0 in F such that $a \oplus 0 = 0 \oplus a = a$ for all a in F.
   - **Inverse Elements**: For each a in F, there exists an element $-a$ in F such that $a \oplus (-a) = 0$.
   - **Commutativity**: For any a, b in F, $a \oplus b = b \oplus a$.
2. **Abelian Group under Multiplication**: The set F^* (which is F excluding the additive identity 0) forms an abelian group under the operation $*$. This means:
   - **Closure**: For any a, b in F^*, the result $a * b$ is also in F^*.
   - **Associativity**: For any a, b, c in F^*, $(a * b) * c = a * (b * c)$.

- **Identity Element**: There exists an element 1 in F^* such that $a * 1 = 1 * a = a$ for all a in F^*.
- **Inverse Elements**: For each a in F^*, there exists an element a^{-1} in F^* such that $a * a^{-1} = 1$.
- **Commutativity**: For any a, b in F^*, $a * b = b * a$.

3. **Distributive Law**: For all a, b, c in F, the following holds:
   - $(a \oplus b) * c = (a * c) \oplus (b * c)$

Example:

- A finite field of order 10 is:
$$F_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$
- A finite field of order 13 is:
$$F_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$
- A finite field of order 1000 is:
$$F_{1000} = \{0, 1, 2, \ldots, 999\}$$

6 Prime Fields

For every prime number p, the set $R_p = \{0, 1, \ldots, p-1\}$ forms a field (denoted by F_p) under mod-p addition and multiplication.

- **mod p Addition**: The addition operation in this field is defined as $(a + b) \mod p$, where a and b are elements of R_p.
- **mod p Multiplication**: The multiplication operation in this field is defined as $(a * b) \mod p$, where a and b are elements of R_p.

7 Elliptic-curve cryptography

7.1 General curve equations:

- **Linear Equation:**
$$y = mx + b \tag{1}$$
This equation represents a straight line, where m is the slope, and b is the y-intercept.
- **Quadratic Equation:**
$$y = ax^2 + bx + c \tag{2}$$
This equation represents a parabola, where a, b, and c are constants.
- **Cubic Equation:**
$$y = ax^3 + bx^2 + cx + d \tag{3}$$
This equation represents a more complex curve, where a, b, c, and d are constants.

7.2 Elliptic Curves

An elliptic curve is defined by the equation:

$$y^2 = x^3 + ax + b \tag{4}$$

where a and b are constants.

For cryptography purpose, the curve must be non-singular, which means it has no cusps or self-intersections. This is ensured by the condition:

$$4a^3 + 27b^2 \neq 0 \tag{5}$$

7.3 Points on the Curve

A point P on the elliptic curve is a pair of coordinates (x, y) that satisfy the curve equation.

For example, if (x, y) fits the equation $y^2 = x^3 + ax + b$, then (x, y) is a point on the curve.

There is also a special point at infinity, denoted O, which acts as the identity element in elliptic curve operations.

7.4 Point Addition

7.4.1 Adding Two Distinct Points

Given two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on the curve, where $P \neq Q$, the sum $R = P + Q$ is another point (x_3, y_3) on the curve. The calculation is as follows:

To calculate the slope λ of the line through P and Q:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \tag{6}$$

To calculate the coordinates of R:

$$x_3 = \lambda^2 - x_1 - x_2 \tag{7}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \tag{8}$$

Example:

Suppose we have points $P = (2, 3)$ and $Q = (4, 1)$ on an elliptic curve defined by $y^2 = x^3 + ax + b$.

1. **Calculate the slope (λ) of the line through P and Q:**

$$\lambda = \frac{1-3}{4-2} = \frac{-2}{2} = -1 \tag{9}$$

2. **Calculate the x-coordinate of R (x_3):**

$$x_3 = \lambda^2 - x_1 - x_2 = (-1)^2 - 2 - 4 = 1 - 6 = -5 \tag{10}$$

3. **Calculate the y-coordinate of R (y_3):**

$$y_3 = \lambda(x_1 - x_3) - y_1 = -1(2 + 5) - 3 = -1(7) - 3 = -7 - 3 = -10 \tag{11}$$

So, the coordinates of $R = P + Q$ are $R = (-5, -10)$.

7.4.2 Doubling a Point

Given a point $P = (x_1, y_1)$ on the curve, the point $R = 2P$ is calculated as follows:

To calculate the slope λ of the tangent to the curve at P:

$$\lambda = \frac{3x_1^2 + a}{2y_1} \tag{12}$$

To calculate the coordinates of R:

$$x_3 = \lambda^2 - 2x_1 \tag{13}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \tag{14}$$

Example

Suppose we have a point $P = (2, 3)$ on an elliptic curve defined by $y^2 = x^3 + ax + b$, and let's assume $a = 1$.

1. **Calculate the slope (λ) of the tangent at P:**

$$\lambda = \frac{3(2)^2 + 1}{2(3)} = \frac{3(4) + 1}{6} = \frac{12 + 1}{6} = \frac{13}{6} \tag{15}$$

2. **Calculate the x-coordinate of R (x_3):**

$$x_3 = \lambda^2 - 2x_1 = \left(\frac{13}{6}\right)^2 - 2(2) = \frac{169}{36} - 4 = \frac{169}{36} - \frac{144}{36} = \frac{25}{36} \tag{16}$$

3. **Calculate the y-coordinate of R (y_3):**

$$\begin{aligned} y_3 &= \lambda(x_1 - x_3) - y_1 \\ &= \frac{13}{6}\left(2 - \frac{25}{36}\right) - 3 \\ &= \frac{13}{6}\left(\frac{72 - 25}{36}\right) - 3 \\ &= \frac{13}{6}\left(\frac{47}{36}\right) - 3 \\ &= \frac{611}{216} - 3 \\ &= \frac{611}{216} - \frac{648}{216} \\ &= \frac{-37}{216} \end{aligned}$$

So, the coordinates of $R = 2P$ are $R = \left(\frac{25}{36}, \frac{-37}{216}\right)$.

ECC operates over finite fields $\mathbb{F}_p$ where p is a prime number. This means all arithmetic operations (addition, subtraction, multiplication, and division) are performed modulo p.

7.5 Example of ECC Operations

Consider the elliptic curve defined by:

$$y^2 = x^3 + 2x + 3 \tag{17}$$

over the finite field $\mathbb{F}_5$ (i.e., modulo 5).

Points on the Curve

Calculate the points on the curve by checking which pairs (x, y) satisfy the equation:

For $x = 0$:

$$y^2 \equiv 3 \mod 5 \quad \text{(No valid } y\text{)} \tag{18}$$

For $x = 1$:

$$y^2 \equiv 1 + 2 + 3 = 6 \equiv 1 \mod 5 \tag{19}$$

$$y = \pm 1 \Rightarrow (1, 1) \text{ and } (1, 4) \tag{20}$$

For $x = 2$:

$$y^2 \equiv 8 \equiv 3 \mod 5 \quad \text{(No valid } y\text{)} \tag{21}$$

For $x = 3$:

$$y^2 \equiv 27 + 6 = 33 \equiv 3 \mod 5 \quad \text{(No valid } y\text{)} \tag{22}$$

For $x = 4$:

$$y^2 \equiv 64 + 8 = 72 \equiv 2 \mod 5 \quad \text{(No valid } y\text{)} \tag{23}$$

So the valid points are: $(1, 1)$ and $(1, 4)$.

Key Generation

Base Point G: Let $G = (1, 1)$.

Private Key k: Choose $k = 2$.

Calculate Public Key

$$K = kG = 2G \tag{24}$$

Doubling the base point $G = (1, 1)$:

$$\lambda = \frac{3(1)^2 + 2}{2(1)} \equiv \frac{5}{2} \equiv \frac{0}{2} = 0 \mod 5 \tag{25}$$

$$x_3 = 0^2 - 2 \cdot 1 \equiv -2 \equiv 3 \mod 5 \tag{26}$$

$$y_3 = 0 \cdot (1 - 3) - 1 \equiv -1 \equiv 4 \mod 5 \tag{27}$$

Thus, $2G = (3, 4)$, and the public key K is $(3, 4)$.