WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205   Email: cypriansakwa@gmail.com

Foundational Mathematics for Web3 Builders

April 22, 2024

Table of Contents i

Table of Contents ii

Symbols

Throughout this course, we employ the following commonly used mathematical symbols:

$\in$ means "belongs to" (or, is an element of);

$\notin$ means "does not belongs to" (or, is not an element of);

Thus, if a is an element of X we write $a \in X$ and if y does not belong to X we write $y \notin X$.

$\Rightarrow$ means "implies that" (or, implies);

: means "such that." We can also use $|$.

1 Basic properties of the integers

Much of modern cryptography is built on the foundations of algebra and number theory. Number Theory is the study of the the integers $\mathbb{Z} = \{\cdots, -4, -3, -2, -1, 0, 1, 2, 3, \cdots\}$. This chapter focuses on some of the basic properties of the integers, such as the notions of divisibility and primality, unique factorization into primes, greatest common divisors, and least common multiples.

1.1 Divisibility and primality

Definition 1

An integer $a \neq 0$ is called a divisor (factor) of an integer b (written $a \mid b$) if $b = ac$ for some $c \in \mathbb{Z}$. We also say that b is a multiple of a, or that b is divisible by a. If a does not divide b, then we write $a \nmid b$.

Example 1

a) $2 \mid 8$ because $8 = 2 \cdot 4$

b) $4 \mid -20$ since $-20 = 4(-5)$

c) $3 \nmid 16$ since when we try to divide 16 by 3 we get a remainder.

The following theorem gives some of elementary divisibility properties.

Theorem 2

Let $a, b, c \in \mathbb{Z}$

a) $a \mid a, \;\; 1 \mid a, \;\; a \mid 0$

b) *If $a \mid b$ and $a \mid c$ then $a \mid (b + c)$ and $a \mid (b - c)$.*

c) *If $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof.

a) From the definition of divisibility, using elementary algebraic properties of the integers we have $a \mid a$ since we can write $a \cdot 1 = a$, $1 \mid a$ because we can write $1 \cdot a = a$, $a \mid 0$ because we can write $a0 \cdot 0$.

b) If $a \mid b$ and $a \mid c$ then there exists integers x and y such that $b = ax$ and $c = ay$. Adding we obtain $b + c = ax + ay$ or $b + c = a(x + y)$ and so $a \mid (b + c)$.
Similarly, subtracting $b - c = ax - ay$ or $b - c = a(x - y)$ hence $a \mid (b - c)$.

c) If $a \mid b$ and $b \mid c$ then there exists integers x and y such that $b = ax$ and $c = by$.
Thus $c = by = (ax)y = a(xy)$ implying that $a \mid c$.

$\square$

Definition 3 (Primes and composites)

If n is a positive integer greater than 1 and no other positive integers besides 1 and n divide n then we say n is prime.
If $n > 1$ but n is not prime, then n is said to be composite. That is, $n \in \mathbb{Z}$ is composite if and only if $n = ab$ for some $a, b \in \mathbb{Z}$.
The first few primes are $2, 3, 5, 7, 11, 13, 17, 19, \cdots$.

Note that the set of primes is infinite.

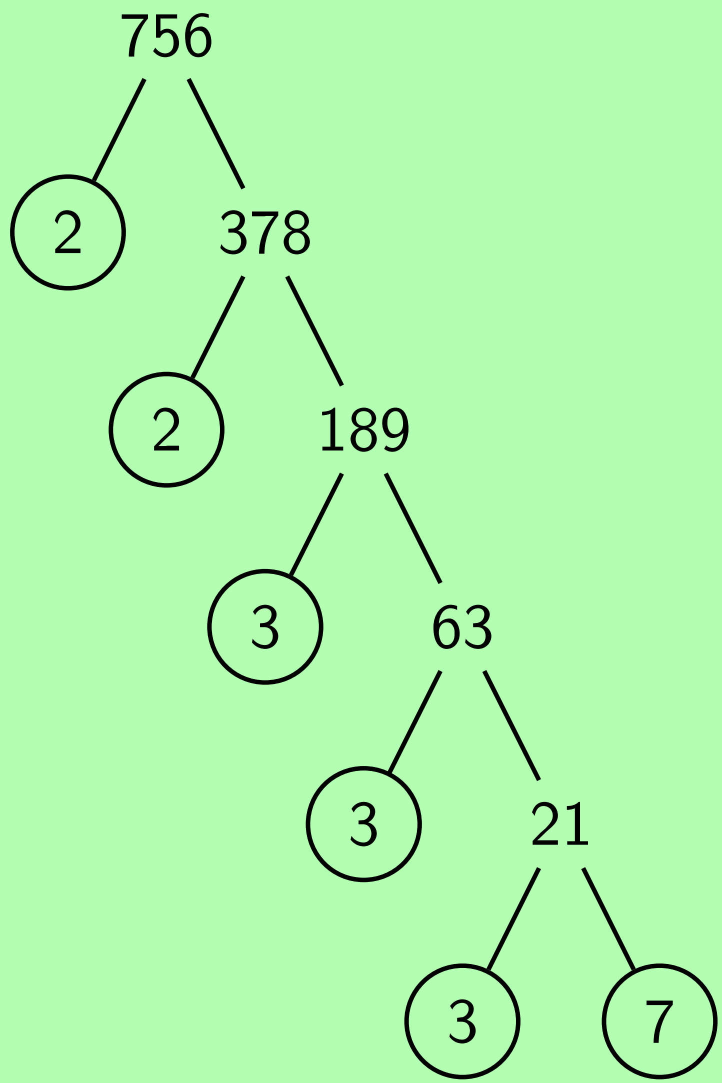
Theorem 4 (Fundamental theorem of arithmetic)

Every integer greater than 1 is either a prime number or it can be factored uniquely into a product of primes.
That is, $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$,
where $p_1, \cdots, p_r$ are distinct primes and $n_1, \cdots, n_r$ are positive integers.

This theorem is also called the unique factorization theorem or unique prime factorization theorem

Example 2

Find the prime factorization for 3780



Thus, $756 = 2^2 \times 3^3 \times 7$

Example 3

Find the prime factorization for 12600

$$\begin{array}{c|l} 2 & 12600 \\ \hline 2 & 6300 \\ \hline 2 & 3150 \\ \hline 3 & 1575 \\ \hline 3 & 525 \\ \hline 5 & 175 \\ \hline 5 & 35 \\ \hline 7 & 7 \\ \hline & 1 \end{array}$$

Thus $12600 = 2^3 \times 3^2 \times 5^2 \times 7$

Note that any algorithm finding prime factorization of integers also answers a simpler question of whether a given integer is prime or composite? Later, in section 13, we will do primality testing using the Fermat's little theorem.

Definition 5

A common divisor of two integers a and b is a positive integer d that divides both of them. When every divisor of a and b is also a divisor of d then we say that d is the greatest common divisor (gcd) of a and b.

For instance, $\pm1,\ \pm2,\ \pm3,\ \pm4,\ \pm6,\ \pm12$ are common divisors of 36 and 60 but 12 is the greatest common divisor.

Example 4

Find the $\gcd(12600, 756)$.
This is left to the learner.

Theorem 6

If a and b are integers with $d = \gcd(a, b)$, then

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Proof.

Suppose $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = c$. Then $c \mid \frac{a}{d}$ and $c \mid \frac{b}{d}$ from the definition of $\gcd$.

This implies that there are integers x and y such that $\frac{a}{d} = cx$ and $\frac{b}{d} = cy$. This implies that $a = cdx$ and $b = cdy$. So, cd is a common divisor of a and b. Since d is the greatest common divisor and $cd \geq d$, we must have $c = 1$. □

There is a fast and efficient method to compute the greatest common divisor of any two integers using repeated division algorithm. This technique of finding the gcd of integers is called as Euclidean algorithm.

1.2 Euclidean algorithm

The Euclidean Algorithm, which allows us to compute $\gcd$ of numbers without factoring, is a very useful algorithms in number theory. For instance, it is useful in cryptographic situations where the numbers often have several hundreds of digits and are hard to factor. Euclidean Algorithm is also called Euclid's algorithm. very important.

Definition 7 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then a divided by b has quotient q and remainder r means that

$$a = b \cdot q + r \quad \text{with} \quad 0 \le r < b.$$

It can be shown that both the quotient and the remainder always exist and are unique, as long as the divisor is not 0. Division algorithm is not actually an algorithm, but this is this theorem's traditional name.

Example 5

34=5×6+4

Suppose we want to find the greatest common divisor of 36 and 60 using division algorithm, divide 36 into 60 and note the quotient q_1 and remainder r_1. Then divide r_1 into q_1 to obtain the new quotient q_2 and new remainder r_2. Continue this process until eventually we get a remainder of 0 as shown below.

Step 1: Apply the division algorithm to 60 and 36.
$60 = 36(1) + 24$

Step 2: Apply the division algorithm to 36 and 24.

$36 = 24(1) + 12$

Step 3: Apply the division algorithm to 24 and 12.

$24 = 12(2) + 0$

The $\gcd(60, 36)$ is the last non-zero remainder and it is 12.

Step 3: Apply the division algorithm to 24 and 12.

$24 = 12(2) + 0$

The $\gcd(60, 36)$ is the last non-zero remainder and it is 12.

To compute the $\gcd$ of two integers by Euclidean algorithm is to find the $\gcd$ by repeated division with remainder as explained above.

Example 6

Use division algorithm to compute $\gcd(12600, 756)$

Solution

$$12600 = 756(16) + 504$$

$$756 = 504(1) + 252$$

$$504 = 252(2) + 0$$

Thus $\gcd(12600, 756) = 252$

Example 7

Compute $\gcd(758, 121)$

Solution

$$758 = 121(6) + 32$$

$$121 = 32(3) + 25$$

$$32 = 25(1) + 7$$

$$25 = 7(3) + 4$$

$$7 = 4(1) + 3$$

$$4 = 3(1) + 1$$

$$3 = 1(3) + 0$$

$$\gcd(758, 121) = 1$$

An integer a is said to be relatively prime to an integer b if $\gcd(a, b) = 1$. We also say that the integers a and b are coprimes. That means that their only common factors are ± 1.

For instance, 11 and 17 are relatively prime.

Euclidean Algorithm: Let a and b be positive integers with $a \geq b$ and $b \neq 0$. To find $\gcd(a, b)$ we use the Euclidean algorithm which consists of a sequence of divisions with remainder as illustrated below.

Algorithm 1

$$
\begin{aligned}
a &= q_1 b + r_1 \quad \text{with } 0 \le r_1 < b \\
b &= q_2 r_1 + r_2 \quad \text{with } 0 \le r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 \quad \text{with } 0 \le r_3 < r_2 \\
r_2 &= q_4 r_3 + r_4 \quad \text{with } 0 \le r_4 < r_3 \\
\vdots \quad & \quad \vdots \\
r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \quad \text{with } 0 \le r_{k-1} < r_{k-2} \\
r_{k-2} &= q_k r_{k-1} + r_k \quad \text{with } 0 \le r_k < r_{k-1} \\
r_{k-1} &= q_k r_k + 0
\end{aligned}
$$

The last non-zero remainder, namely r_k, is $\gcd(a, b)$.

1.3 The Extended Euclidean Algorithm

In order to perform computations in modular arithmetic (studied in the next chapter), we have to get familiar with the Extended Euclidean Algorithm.

The Euclidean Algorithm yields a very useful fact that the $\gcd(a, b)$ can be expressed as a linear combination of a and b. That is, there exist integers x and y such that $\gcd(a, b) = ax + by$. For instance, the gcd of 10 and 4 is 2 and the equation $10x + 4y = 2$ has a solution $(x, y) = (1, -2)$ meaning that $10(1) + 4(-2) = 2$.

Similarly, the gcd of 195 and 42 is 3 and the equation $195x+42y = 3$ has a solution $(x, y) = (-3, 14)$ and so $195(-3) + 42(14) = 3$.

The method for obtaining x and y is called the Extended Euclidean Algorithm.

Writing $\gcd(a, b) = ax + by$

Beginning with second last line of algorithm 1 we make the $\gcd$ r_k the subject of the equation and substitute for r_{k-1} using the third last equation as follows.

$r_k = r_{k-2} - q_k r_{k-1} = r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2})$.

We then substitute for r_{k-2} and simplify. Then substitute for r_{k-3} and simplify. We continue until we eventually substitute for r_1 and simplify. This yields $r_k = ax + by$

Example 8

Find $\gcd(765, 364)$ and express it in the form $765x + 364y$

Solution

Using Euclidean Algorithm we get

$$765 = 364(2) + 37$$

$$364 = 37(9) + 31$$

$$37 = 31(1) + 6$$

$$31 = 6(5) + 1$$

$$6 = 1(6) + 0$$

Thus $\gcd(765, 364) = 1$

Since 1 is the $\gcd$, we apply the extended Euclid's algorithm by first making 1 in second last equation the subject of the formula. Then substituting all the remainders one at a time from bottom going up.

Solution (conti...)

$$\begin{aligned}1 &= 31 - 6(5)\\ &= 31 - [37 - 31(1)](5) = 31 - 37(5) + 31(5) = -37(5) + 31(6)\\ &= -37(5) + [364 - 37(9)](6) = -37(5) + 364(6) - 37(54)\\ &= 364(6) - 37(59) = 364(6) - [765 - 364(2)](59)\\ &= 364(6) - 765(59) + 364(118) = -765(59) + 364(124)\end{aligned}$$

Thus $1 = 765(-59) + 364(124)$.

Example 9

Use the Euclidean algorithm to find $d = \gcd(60, 33)$. Write d in the form $d = 60n + 33m$ where n and m are integers.

Solution

Using Euclidean Algorithm we get

$$60 = 33(1) + 27$$

$$33 = 27(1) + 6$$

$$27 = 6(4) + 3$$

$$6 = 3(2) + 0 \text{ Thus, } d = 3$$

Now, making $\gcd$ the subject of the equation and substituting the remainders one after the other we obtain the following

$$3 = 27 - 6(4) = 27 - [33 - 27(1)](4)$$

$$= 27 - 33(4) + 27(4) = -33(4) + 27(5)$$

$$= -33(4) + [60 - 33(1)](5) = -33(4) + 60(5) - 33(5)$$

$$= 60(5) + 33(-9)$$

1.4 Number Bases

In this section we consider various number systems and see how to convert from one system to the other. The system in every day use is the decimal (denary) system which uses digits $0, 1, 2, 3, 4, \cdots, 9$ and has a base or radix of 10. This system has radix (base) 10. Computers are based on a binary system. The binary system uses the digits 0 and 1 only and has a base or radix of 2.

We convert a number from base 10 to any other base with the use of the Division Algorithm. For instance, we convert a denary number to binary by repeatedly dividing it by 2 and noting the remainder at every stage. This continues until the quotient is 0.

Example 10

Convert a decimal number 53 to binary.

Solution

Using division algorithm, we get

$$\begin{aligned}
53 &= 26(2) + 1 \\
26 &= 13(2) + 0 \\
13 &= 6(2) + 1 \\
6 &= 3(2) + 0 \\
3 &= 1(2) + 1 \\
1 &= 0(2) + 1
\end{aligned}$$

Writing the remainders from bottom going up gives 110101_2. Thus $53_{10} = 110101_2$.
Subscripts tell the base the number is in.

Fractional denary numbers can be converted to binary by repeatedly multiplying by 2 till 1.0 is obtained.

Example 11

Convert 0.8125_{10} to binary.

Solution

$$
\begin{aligned}
0.8125 \times 2 &= 1.625 \\
0.625 \times 2 &= 1.25 \\
0.25 \times 2 &= 0.5 \\
0.5 \times 2 &= 1.0
\end{aligned}
$$

Writing the circled from up going down gives 1101.

Thus $0.8125_{10} = 0.1101_2$.

The Octal number system uses the digits $0, 1, 2, 3, \cdots, 7$ only and has a base or radix of 8

Example 12

Convert 686_{10} to octal.

Solution

By division algorithm, we have

$$\begin{aligned} 686 &= 85(8) + 6 \\ 85 &= 10(8) + 5 \\ 10 &= 1(8) + 2 \\ 1 &= 0(8) + 1 \end{aligned}$$

Writing the remainders from bottom going up gives 1256_8.
Thus $686_{10} = 1256_8$

Fractional denary numbers can be converted to octal numbers by repeatedly multiplying by 8 till a whole number is obtained.

Example 13

Convert 0.978515625_{10} to octal.

Solution

$$0.978515625 \times 8 = 7.828125$$

$$0.828125 \times 8 = 6.625$$

$$0.625 \times 8 = 5.0$$

Writing the circled from up going down gives 765.

Thus $0.978515625_{10} = 0.765_8$.

Example 14

Convert the base 10 number 1292 to a base 7 number.

Solution

Using division algorithm, we get

$$
\begin{aligned}
1292 &= 184(7) + 4 \\
184 &= 26(7) + 2 \\
26 &= 3(7) + 5 \\
3 &= 0(7) + 3
\end{aligned}
$$

Thus $1292_{10} = 3524_7$

Hexadecimal number system uses the digits $0, 1, 2, 3, \cdots, 9, A, B, C, D, E, F$ only where A corresponds to 10 and B to 11 and so on. It has a base or radix of 16. We convert a denary number to Hexadecimal number by repeatedly dividing it by 16 and noting the remainder in every stage.

Example 15

Convert 43928_{10} to Hexadecimal.

Solution

$$43928 = 2745(16) + 8$$

$$2745 = 171(16) + 9$$

$$171 = 10(16) + 11 = B$$

$$10 = 0(16) + 10 = A$$

Thus $43928_{10} = AB89_{16}$

Fractional denary numbers can be converted to hexadecimal numbers by repeatedly multiplying by 16 till a whole number is obtained.

Example 16

Convert 0.478759765625_{10} to Hexadecimal.

Solution

$$
\begin{aligned}
0.478759765625 \times 16 &= 7.66015625 \\
0.66015625 \times 16 &= 10.5625 \\
0.5625 \times 16 &= 9.0
\end{aligned}
$$

Writing the circled from up going down gives $7A9$.

Thus $0.478759765625_{10} = 0.7A9_{16}$.

To convert a number from another base to base 10 use place-value notation, multiply each digit of the number by the base raised to the power of its position, starting from the rightmost position and moving left. Then sum up all these products. Recall that in 723.56, the 7 represents 7×10^2, the 2 represents 2×10^1, the 3 represents 3×10^0, the 5 represents 5×10^{-1} and the 6 represents 6×10^{-2} so that

$$723.56 = 7 \times 10^2 + 2 \times 10^1 + 3 \times 10^0 + 5 \times 10^{-1} + 6 \times 10^{-2}$$

Example 17

Convert the binary number 11101.11 to decimal.

Solution

$$1 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 + 1 \times 2^{-1} + 1 \times 2^{-2} = 29.75$$

Example 18

Convert the octal number 157.6 to decimal.

Solution

$1 \times 8^2 + 5 \times 8^1 + 7 \times 8^0 + 6 \times 8^{-1} = 111.75$

Example 19

Convert 3523_7 to base 10 number.

Solution

$3523 = 3{\cdot}7^3+5{\cdot}7^2+2{\cdot}7^1+3{\cdot}7^0 = 3{\cdot}343+5{\cdot}49+2{\cdot}7+3{\cdot}1 = 1291_{10}.$

Example 20

Convert $15A_{16}$ to decimal.

Solution

$1 \times 16^2 + 5 \times 16^1 + 10 \times 16^0 = 346_{10}$

Example 21

Convert $1A5C.2_{16}$ to denary.

Solution

$1 \times 16^3 + 10 \times 16^2 + 5 \times 16^1 + 12 \times 16^0 + 2 \times 16^{-1} = 6748.125_{10}$.

Thus $1A5C.2_{16} = 6748.125_{10}$.