WEB3CLUBS FOUNDATION LIMITED

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

Foundational Mathematics for Web3 Builders

Lecture 2

April 23, 2024

Exercise 1

1. Use the Euclidean algorithm to compute each of the following gcd's.

   a) $\gcd(4115, 22630)$ b) $\gcd(217284, 39504)$

2. Write a program to compute the greatest common divisor $\gcd(a, b)$ of two integers a and b. Ensure that your program works even if either a or b is zero. Make sure that you don't go into an infinite loop if a and b are both zero.
3. A number L is called a common multiple of m and n if both m and n divide L. The smallest such L is called the least common multiple of m and n and is denoted by LCM(m, n). For example, $LCM(3, 5) = 15$ and $LCM(24, 36) = 72$.

   a) Find the following least common multiples:

      i) LCM$(12, 30)$ ii) LCM$(10, 20)$ iii) LCM$(60, 180)$

Exercise (conti....)

b) For each of the LCMs that you computed in (a), compare the value of LCM(m, n) to the values of m, n, and $\gcd(m, n)$. Try to find a relationship.

c) Use your result in (b) to compute LCM$(816, 936)$.

Exercise 2

1. Find a solution in integers to the following equations

   a) $18107x + 3292y = \gcd(18107, 3292)$

   b) $24690x + 135780y = \gcd(24690, 135780)$

2. Implement the extended Euclidean algorithm on your computer to compute the greatest common divisor g of the positive integers a and b together with a solution (x, y) in integers to the equation $ax + by = \gcd(a, b)$.

3. Use your above program to compute $g = \gcd(a, b)$ and integer solutions to $ax + by = g$ for the following pairs (a, b).

   a) $(9954, 810)$ b) $(5835, 2505)$ c) $(1452, 550)$

   d) $(22241739, 19848039)$ e) $(63750, 16774)$ f) $(2827, 3364)$

4. What happens to your program if $b = 0$? Fix your program so that it deals with this case correctly.

Exercise (Conti...)

5. Note that if (x, y) is a solution then $(x + b, y - a)$ will also be a solution. With is in mind, modify your program so that it always returns a solution with $x > 0$.

1.5 Modular arithmetic

There are many applications of modular arithmetic in computer science. Some of the applications include the construction of pseudo-random number generators, hashing Functions and Cryptology.

Definition 8

Let m be a positive integer. We say that the integers a and b are congruent modulo m (or $\mathrm{mod} m$) if $m \mid (a - b)$ and we write $a \equiv b (\mathrm{mod}\ m)$. If $m \nmid (a - b)$, then we write $a \not\equiv b (\mathrm{mod}\ m)$.

The relation $a \equiv b (\mathrm{mod}\ m)$ is a congruence relation, or simply, a congruence. The number m is called the modulus of the congruence. Two numbers are are said to be incongruent with respect to a given modulus m if they are not congruent with respect to that modulus m.

Example 22

a) $10 \equiv 4 (\bmod 3)$ since $3 \mid (10 - 4)$

b) $10 \equiv 1 (\bmod 3)$ since $3 \mid (10 - 1)$

c) $15 \equiv -5 (\bmod 3)$ since $4 \mid (15 - -5)$ or $4 \mid 20$

d) $22 \not\equiv 4 (\bmod 5)$ since $5 \nmid 18$

Given $a, b, m \in \mathbb{Z}$ with $m > 0$, we also say that b is congruent to $a \mod m$ if $b = a + mt$ for some integer t.

Example 23

Which numbers are congruent to $3 \mod 7$?

Solution

From above, $a \equiv 3 \mod 7$ if $a = 6 + 7t$ for some integer t. Taking $t = \cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots$ we get
$\{\cdots, -25, -18, -11, -4, 3, 10, 17, 24, 31, \cdots\}$
Notice that all these numbers leave a remainder of 3 on division by 7.

Definition 9

Given integers a and m, with $m > 0$, $a \bmod m$ is defined to be the remainder when a is divided by m.

Example 24

a) $14 \bmod 5 = 4$

b) $139 \bmod 10 = 9$

c) $-14 \bmod 5 = 1$

d) $1148 \bmod 5 = 3$

e) $-4 \bmod 9 = 5$

f) $(17 + 23) \bmod 5 \equiv 2 + 3 = 0$

g) $(18 + 23) \bmod 4 \equiv 2 + 3 = 1$

h) $(19 \times 288) \bmod 5 \equiv 4 \times 3 \equiv 12 \bmod 5 = 2$

i) $(11^2 \times 13^3) \bmod 4 \equiv (3^2 \times 1^3) \bmod 4 \equiv 1 \times 1 = 1$

Example 25

Calculate the remainder of 35^{2024} on division by 17.

Solution

First reduce $35 \bmod 17 = 1 \bmod 17$.

Thus $35^{2024} \bmod 17 = 1^{2024} \bmod 17 = 1$.

So when 35^{2024} is divided by 17 the remainder is 1.

Example 26

Find $27^{1001} \bmod 14$

Solution

First, $27 \bmod 14 \equiv 13 \bmod 14 \equiv -1 \bmod 14$.

Therefore, $27^{1001} = (-1)^{1001} = -1 \bmod 14$

Since $-1 \equiv 13 \bmod 14$, the remainder is 13.

1.6 Fast powering algorithm

The fast powering algorithm, also known as exponentiation by squaring algorithm, is a technique used to efficiently compute the power of a number, especially in modular arithmetic. Some texts call it Square-and-Multiply Algorithm. This algorithm greatly reduces the number of multiplications needed compared to the straightforward method of multiplying the base by itself repeatedly.

In some cryptosystems that we will study, for example the RSA we will be required to compute large powers of a number b modulo another number m and so the fast powering algorithm combined with Fermat's Little Theorem or Euler's Theorem will be very vital

This algorithm works as follows;

To find n^k we do the following

We start with n and square it repeatedly to find the sequence

$$n,\ n^2,\ n^4,\ n^8,\ n^{16}, \cdots$$

then select the terms in the sequence that multiply to give n^k. We can also saying that we came up with the above sequence by finding n^{2^i} where $i = 0, 1, 2, 3, \cdots$

Notice that it is relatively easy to compute the above sequence of values since each number in the sequence is the square of the preceding one.

Example 27

Find $2^{71} \bmod 9$

Solution

Let us find 2^{2^i} where $i = 0, 1, 2, 3, \cdots 6$.

$$\begin{array}{llll} 2^1 = 2 & 2^4 = 16 = 7 & 2^{16} = 7 & \\ & & & 2^{64} = 7 \\ 2^2 = 4 & 2^8 = 4 & 2^{32} = 4 & \end{array}$$

Therefore,

$$\begin{aligned} 2^{71} &= 2^{64+4+2+1} \\ &= 2^{64} \times 2^4 \times 2^2 \times 2^1 \\ &= 7 \times 7 \times 4 \times 2 = 5 \end{aligned}$$

Some explanation on the above solution. How did we know that we were going to find 2^{2^i} with $i = 0, 1, 2, 3, \cdots 6$? So how did we know that we were going to square 7 times? The simple answer is that the exponent 71 when converted to binary gives us binary number 1000111 which has 7 digits.

Example 28

Compute $3^{265} \bmod 17$

Solution

For us to tell how many times we would square we need to convert the exponent 265 to binary to get 100001001 which has 9 digits so we will find 3^{2^i} with $i = 0, 1, 2, 3, \cdots, 8$.

Let us use a table to make this clarify.

i	0	1	2	3	4	5	6	7	8
$3^{2^i} \bmod 17$	3	9	13	16	1	1	1	1	1

This table means

$$\begin{array}{lll} 3^1 = 3 & 3^8 = 16 & 3^{64} = 1 \\ 3^2 = 9 & 3^{16} = 1 & 3^{128} = 1 \\ 3^4 = 13 & 3^{32} = 1 & 3^{256} = 1 \end{array}$$

To get $3^{265} \bmod 17$ we can combine a few of the squares.

Let us pick $3^{16} = 1$.

Solution (conti...)

By division Algorithm, we have $265 = 16 \cdot 16 + 9$.

$$\begin{aligned}3^{265} &= 3^{16\cdot 16+9}\\ &= \left(3^{16}\right)^{16} \times 3^9\\ &= 1 \times 3^9\\ &= 3^9 = 3^8 \times 3^1\\ &= 16 \times 3\\ &= 14\end{aligned}$$

Example 29

Find the remainder of 12^{2024} on division by 17

Solution

We apply fast powering algorithm.

$$\begin{aligned} 12^1 &= 12 \\ 12^2 &= 8 \\ 12^4 &= 13 \\ 12^8 &= 16 \\ 12^{16} &= 1 \end{aligned}$$

The result $12^{16} = 1$ has made our working easier since we know that raising 1 to any power will give us 1.
Therefore, by division algorithm $2024 = 16 \cdot 126 + 8$.
Thus, $\begin{aligned}[t] 12^{2024} &= 12^{16\cdot126+8} \\ &= \left(12^{16}\right)^{126} \times 12^8 \\ &= 1^{126} \times 16 \\ &= 16 \end{aligned}$

Example 30

Calculate the remainder of 24^{62} on division by 11.

Solution

First reduce $24 \mod 11 = 2 \mod 11$.

Thus, $24^{62} \mod 11 = 2^{62} \mod 11$

Since 2 and 11 are relatively prime, we can find a smaller power of 2 which is congruent to $\pm 1 \mod 11$.

Let us find powers of 2 to get that smaller power we are looking for.

$2^2 = 4 \mod 11$

$2^3 = 8 \mod 11$

$2^4 = 5 \mod 11$

$2^5 = 10 = -1 \mod 11$

We have that $2^5 = -1 \mod 11$ but we require $2^{62} \mod 11$

Applying division algorithm on 62 and 5 we get $62 = 5 \cdot 12 + 2$.

Solution (conti...)

Thus,

$$\begin{aligned} 2^{62} &= 2^{5\cdot 12+2} \\ &= \left(2^5\right)^{12} \times 2^2 \\ &= 1^{12} \times 2^2 \\ &= 4 \end{aligned}$$

Example 31

Find the remainder of $20^{62} + 55^{99}$ on division by 17.

Solution

We calculate $20^{62} \bmod 17$ and $55^{99} \bmod 17$ separately using the strategy from the previous examples then add the results.

First, $20^{62} \bmod 17 \equiv 3^{62} \bmod 17$

Solution (conti...)

Now find powers of $3 \bmod 17$

$3^2 = 9$

$3^3 = 10$

$3^4 = 13$

$3^5 = 5$

$3^6 = 15$

$3^7 = 11$

$3^8 = 16 = -1$

We use $3^8 = 16 = -1$. Since $62 = 8 \cdot 7 + 6$, we have

$$\begin{aligned} 3^{62} &= 3^{8\cdot 7+6} \\ &= \left(3^8\right)^7 \times 3^6 \\ &= (-1)^7 \times 3^6 \\ &= -1 \times 15 = -15 \equiv 2 \bmod 17 \end{aligned}$$

Thus $20^{62} \bmod 17 = 2 \bmod 17$

Solution (conti...)

Now let us calculate $55^{99} \bmod 17 = 4^{99} \bmod 17$

Since $4^2 = 16 \equiv -1 \bmod 17$ and $99 = 2 \cdot 49 + 1$, we have

$$\begin{aligned} 4^{99} &= 4^{2\cdot 49+1} \\ &= \left(4^2\right)^{49} \times 4^1 \\ &= (-1)^{49} \times 4^1 \\ &= -1 \times 4 \\ &= -4 \bmod 17 = 13 \bmod 17 \end{aligned}$$

Thus $55^{99} \bmod 17 = 13 \bmod 17.$

Therefore, $\left(20^{62} + 55^{99}\right) \bmod 17 = 2 + 13 = 15 \bmod 17.$

This method of finding powers of integers modulo p is a longer with bigger powers. In section 11 and section 14 we will look at a reasonably efficient method for computing powers of integers modulo p. The proof of the following theorem if left to the learner