11464: INFORMATION SYSTEMS SECURITY

Chapter 5: Number Theory

Number Theory

By

Mustafa Al-Fayoumi

The language of numbers

- **Natural numbers:**
  - The history of mathematics begins with numbers that were used for counting things and adding things like sacks of grain, cattle in a field and fish in a pond. These numbers are called **natural numbers** or sometimes **counting numbers.** They are all the whole positive numbers greater than zero. Mathematically we can write these numbers as:
    - 1, 2, 3, … , **n**
  - where the three dots (…) mean a continuing sequence up to **n**. For the natural numbers **n** has no upper limit
- **Set:**
  - When we define numbers in this way it is useful to refer to them as a set of numbers. For example, Natural numbers are the set of **whole numbers** greater than 0

The language of numbers

- **Integer:**
  - Integers are the set of **negative and positive whole numbers including zero**. Mathematically we can write these numbers as:
    - **−n**, … , −3, −2, −1, 0, 1, 2, 3, … , **n**
    - where **n** has no upper limit and **−n** has no lower limit
- **Subset:**
  - From this I hope you can see that natural numbers are a subset of integers (where a subset is a set **contained within a larger set**). That is, **every natural number is also an integer, but every integer is not always a natural number**

The language of numbers

- **Factor:**
  - When one number **divides exactly into another number leaving no remainder** it is said to be a factor of that number
  - Mathematically we can express this as:
    - **a** | **b** (**a** is a factor of **b**)
  - A natural number may have several factors. **For example**, 12 has factors 1, 2, 3, 4, 6 and 12 since all of these will divide it exactly leaving no remainder

The language of numbers

- **Activity 5 (self-assessment)**
  - **What are the factors of the following?**
    - **9 : 1, 3, 9**
    - **15 : 1, 3, 5, 15**
    - **17 : 1, 17**
    - **32 : 1, 2, 4, 8, 16, 32**
- **Notes:**
  - You should notice that in every case:
    - one of the factors was always 1
    - every natural number is a factor of itself
    - every natural number has at least two factors (1 and itself)
  - These rules apply for **any** natural number with the exception of 1. (The number 1 is unique in that it has only the single factor of 1)

Prime Numbers

- **Prime numbers** are characterized by the uniqueness of their factorization. **A Prime number** has only two factors: 1 and itself
  - **An example** of prime numbers is 7
    - The only possible factorisation is $7 = 7 \times 1$.
  - **Another example** is 5: it will only factorise as 5×1.

Can we consider the number "6" as prime? "10"?

Compound Numbers

- When it is not prime, the number is said to be a "**compound number**"
- **A compound number** has always more than two factors: 1, itself, and other factor(s).
  - **Example:** 6 is not a prime number because it will factorise as both 3 × 2 and 6 × 1.
    - In other words, 6 has more than 2 factors (1, 2, 3 and 6)
  - **Other example:** 10 is not a prime number, because it will factorise as both 5 × 2 and 10 × 1.
    - In other words, 10 has more than 2 factors (1, 2, 5 and 10)

Prime Factorization

- A factorisation is said to be a "**prime factorisation**" when all the factors are prime numbers.
- **Each numbers has only one unique prime factorisation.**
- **For example,** the number 12 has several factorisations:
  - 12 = 4x3 ; 12 = 6x2 ; 12= 2 x 2 x 3
  - But only one is a "prime factorisation", that is 2 x 2 x 3.
    - All the factors are prime numbers.
- **Other Examples:**
  - $18 = 2 \times 3 \times 3$; $24 = 2 \times 2 \times 2 \times 3$; $40 = 2 \times 2 \times 2 \times 5$; $85 = 5 \times 17$

How we can find the prime factorization of a given number?

Finding the prime factorization

- **Finding the prime factorisation of a number:**
  - To find the prime factorisation of a number X, this number is successively divided by all the prime numbers that are smaller than itself starting with 2 then 3, then 5, and so on…
- Consider S={2 , 3, 5, …} the set of prime numbers less than X (sorted)
- The algorithm works as follows:
  1. Initiation: i=1.
  2. while X>1
  3. Calculate (X mod S[i]) *// This is the remainder of X/S[i]*
     - If the remainder is 0 *// S[i] is a factor*
       - Store S[i];
       - X = X/S[i];
       - Go to step 2
     - Else *// the remainder is not 0, so, S[i] is not a prime factor*
       - i=i+1;
       - Go to step 2
     - End While loop

Finding the prime factorization

- **Example:** Find the prime factorisation of the number 48
- The set of prime numbers less than 48 is S={2, 3, 5, 7, 11, 13, 17, 19, 23, 29 , 29, 31, 37, 41, 43, 47}

48 | 2	remainder 0	So **2 is a factor**
24 | 2	remainder 0	So **2 is a factor**
12 | 2	remainder 0	So **2 is a factor**
6 | 2	remainder 0	So **2 is a factor**
3 | 2	remainder 1	So move to the next prime number
3 | 3	remainder 0	So **3 is a factor**
1	stop dividing since X=1.	

- The prime factorisation of 48 is: 48 = 2x2x2x2x3.

Divisibility

- We say that a nonzero b **divides** a if $a = mb$ for some m, where a, b, and m are integers
- b divides a if there is no remainder on division
- The notation $b \mid a$ is commonly used to mean b divides a
- If $b \mid a$ we say that b is a **divisor** of a

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24
$13 \mid 182$; $-5 \mid 30$; $17 \mid 289$; $-3 \mid 33$; $17 \mid 0$

Properties of Divisibility

- If $a \mid 1$, then $a = \pm 1$
- If $a \mid b$ and $b \mid a$, then $a = \pm b$
- Any $b \neq 0$ divides 0
- If $a \mid b$ and $b \mid c$, then $a \mid c$

$11 \mid 66$ and $66 \mid 198 = 11 \mid 198$

- If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$ for arbitrary integers m and n
- If b g, then g is of the form $g = b * g1$ for some integer $g1$.
- If b h, then h is of the form $h = b * h1$ for some integer $h1$.

Division Algorithm

- *Theorem*:
- Given integers a and n, with n > 0, there exist unique integers q and r satisfying, a = qb + r ; 0 r < b: The integers q and r are called, respectively, the quotient and remainder in the division of a and n, The relationship between these four integers can be shown as

$$a = q \times n + r \qquad\qquad 0 \leq r < n;\ q = [a/n]$$

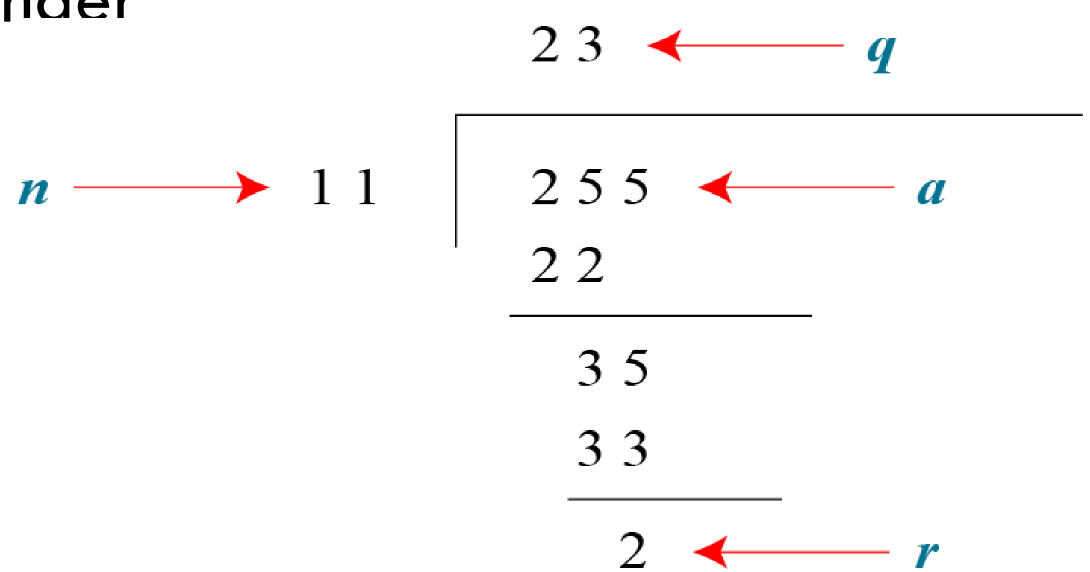
- Example : If a = 592; n = 7

then 592 = 84(7) + 4 then q = 84 and r = 4.

Division Algorithm

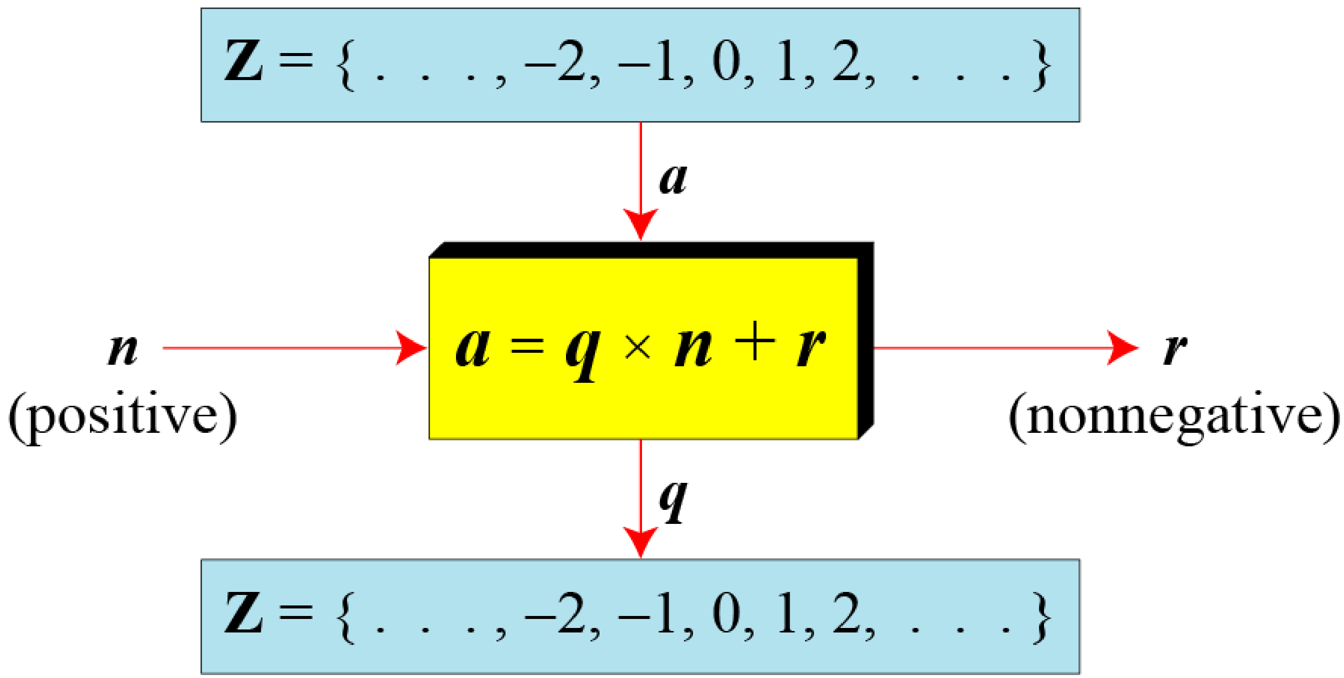
Example 1

- Assume that a = 255 and n = 11. We can find q = 23 and R = 2 using the division algorithm.
- Figure 2.3 Example 2.2, finding the quotient and the remainder



Division Algorithm

Figure 1 Division algorithm for integers



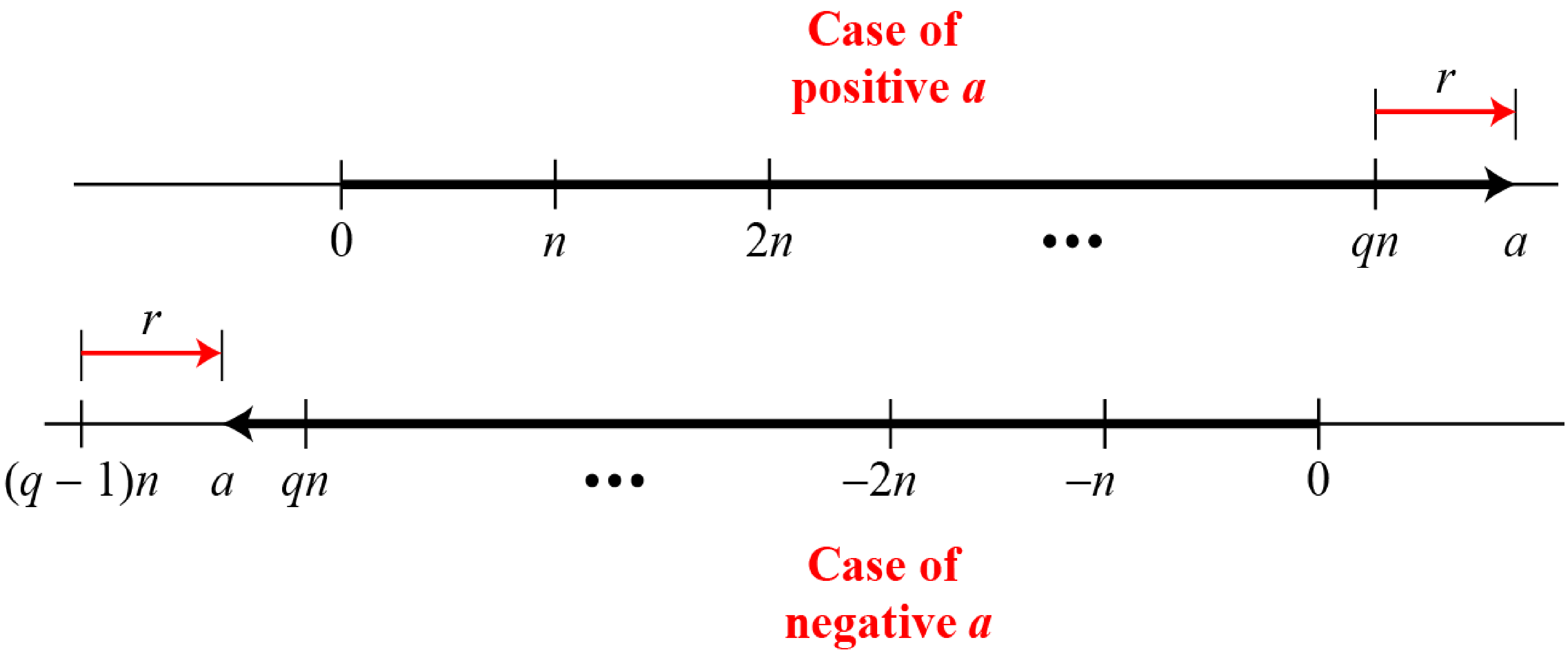
Division Algorithm

Example 2

- When we use a computer or a calculator, r and q are negative when a is negative. How can we apply the restriction that r needs to be positive? The solution is simple, we decrement the value of q by 1 and we add the value of n to r to make it positive.

$$-255 = (-\mathbf{23} \times 11) + (-\mathbf{2}) \quad \leftrightarrow \quad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$

Division Algorithm

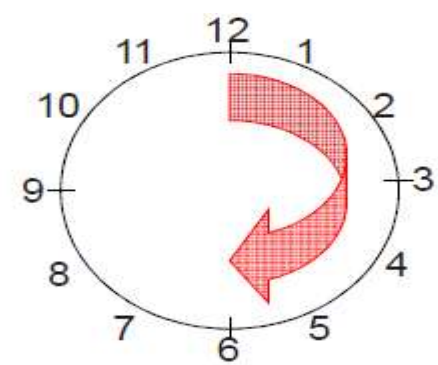


Introduction to Modular Arithmetic

- **Other names for modular arithmetic:**
  - It is also referred to as **modulo arithmetic**, **clock arithmetic** or **remainder arithmetic**. It usually involves concept of full rotation (**circular**) as will be clear later on
- **Set:**
  - A **set** is a **collection of objects**
- **Modulus:**
  - The **size** (that is, **the number of**, say, integers a set contains) is known as the **modulus**

Introduction to Modular Arithmetic

- Generally speaking, most cryptosytems are based on **sets of numbers** that are
  1. **discrete** (sets with integers are particularly useful)
  2. **finite** (i.e., if we only compute with a finiely many numbers)
- Seems too abstract? --- Let's look at a finite set with discrete numbers we are quite familiar with: a clock.



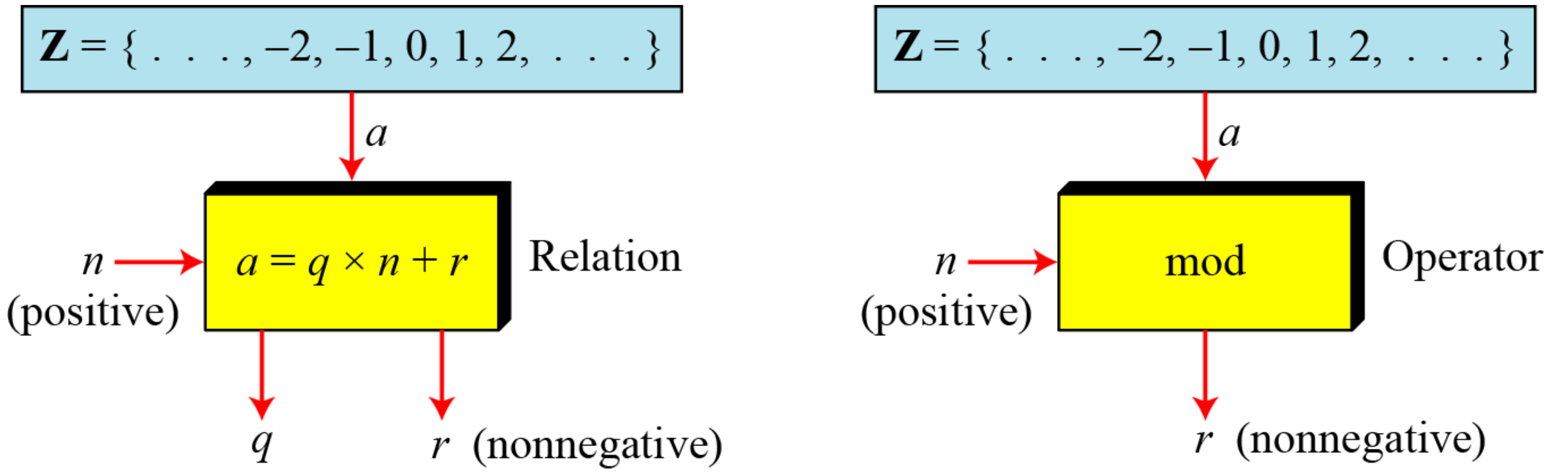
- Interestingly, even though the numbers are incremented every hour we never leave the set of integers:
- 1, 2, 3, … 11, 12, 1, 2, 3, … 11, 12, 1, 2, 3, …:

Modular Arithmetic

- The division relationship ($a = q \times n + r$) discussed in the previous section has two inputs (a and n) and two outputs (q and r). In modular arithmetic, we are interested in only one of the outputs, the remainder r.

- The modulo operator is shown as mod. The second input (n) is called the modulus. The output r is called the residue.

Figure 2.9 ***Division algorithm and modulo operator***



Example 2.14

- Find the result of the following operations:
- a. 27 mod 5 b. 36 mod 12
- c. −18 mod 14 d. −7 mod 10
- Solution
  a. Dividing 27 by 5 results in r = 2
  b. Dividing 36 by 12 results in r = 0.
  c. Dividing −18 by 14 results in r = −4. After adding the modulus r = 10
  d. Dividing −7 by 10 results in r = −7. After adding the modulus to −7, r = 3.

Modular Arithmetic

- Example:

  $a = qn + r \qquad 0 \le r < n; q = \lfloor a/n \rfloor$

  - a = 59; n = 7; 59 = (8)*7 + 3 r = 3; q = 8
  - a = -59; n = 7; -59 = (-9)*7 + 4 r = 4; q = -9
  - 59 mod 7 = 3
  - -59 mod 7 = 4
- Modulo of a negative number
- **-a mod n = n – (a mod n)**
- Example -100 mode 8 = 8 – (100 mod 8) = 8 – 4 = 4
- Example -59 mode 7 = 7 – (59 mod 7) = 7 – 1=3 = 4
- Example -11 mod 7 = 7 – (11 mode 7) = 7 -4 = 3
- Example -17 mode 5 = 5 – (17 mode 5) = 5- 2 = 3
- Example -144 mod 5 = 5 – (144 mod 5) = 5 – 4 = 1
- Example -2 mod 5 = 5 – (2 mod 5) = 5- 2 = 3
- Example -340 mod 60 = 60 – (340/60) = 60 – 40 = 20
- Example -33 mod 26 = 26 – (33 mod 26) = 26 – 7 = 19
- Example -7 mod 26 = 26 – (7 mod 26) = 26 -7 = 19
- Example -54 mod 5 = 5 – (54 mod 5) = 5 – 4 =1

Set of Residues

- The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Z_n.

Figure 2.10 Some Z_n sets

$$\mathbf{Z}_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$$

$$\mathbf{Z}_2 = \{ 0, 1 \} \quad \mathbf{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \} \quad \mathbf{Z}_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$$

$a = 11;$	$n = 7;$	$11 = 1 \times 7 + 4;$	$r = 4$	$q = 1$
$a = -11;$	$n = 7;$	$-11 = (-2) \times 7 + 3;$	$r = 3$	$q = -2$

If ***a*** is an integer and ***n*** is a positive integer, we define ***a mod n*** to be the remainder when ***a*** is divided by ***n***. The integer ***n*** is called the **modulus**. Thus, for any integer ***a***, we can always write:

$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

$11 \bmod 7 = 4;$	$-11 \bmod 7 = 3$

Congruent Modulo (Equivalency Modulo)

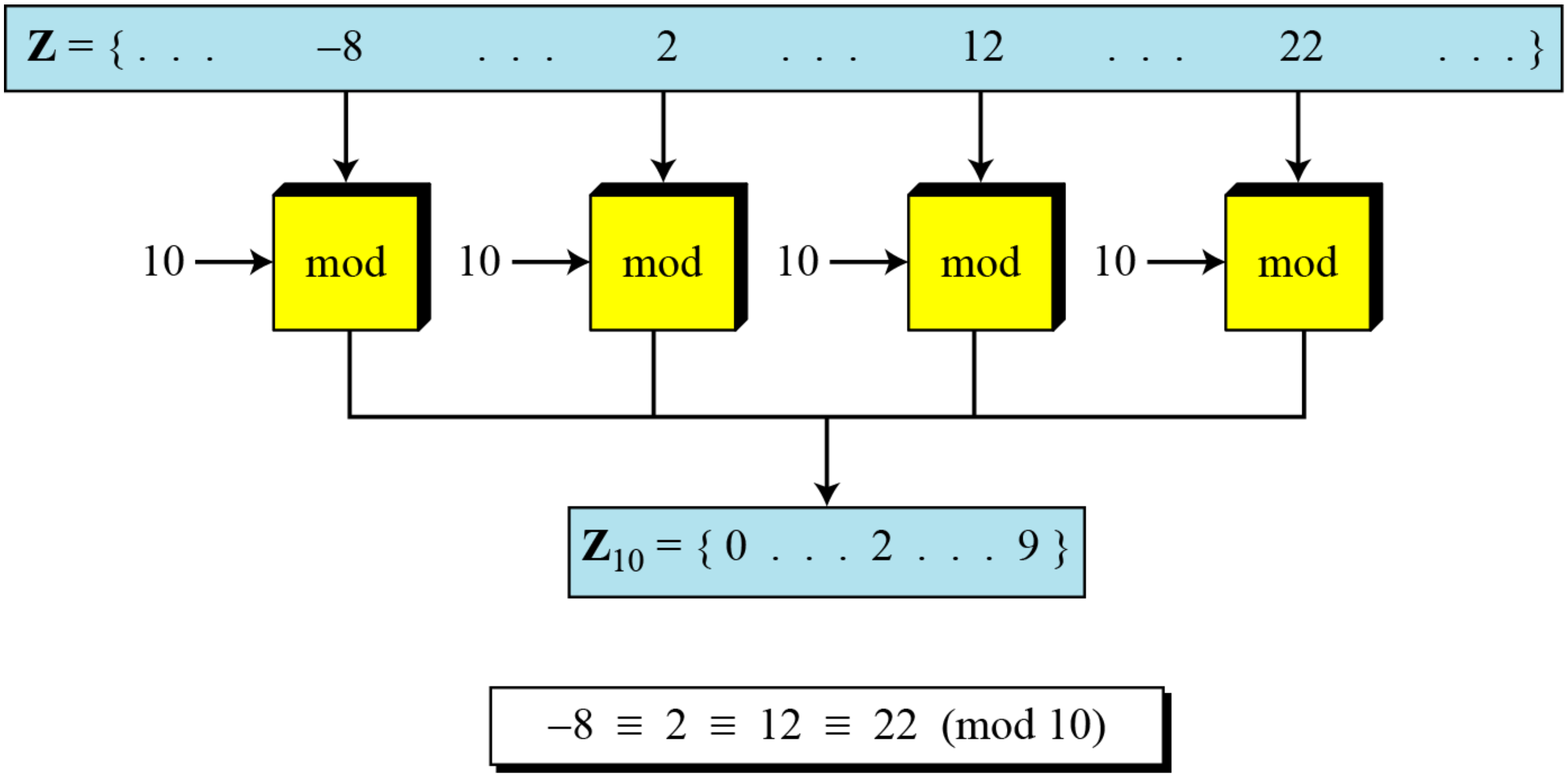
- To show that two integers are congruent, we use the congruence operator (≡). For example, we write:
- Two integers *a* and *b* are said to be **congruent (modulo *n***, if (***a* mod *n***) = (***b* mod *n***). This is written as

$$a \equiv b \pmod{n}.$$

$73 \equiv 4 \pmod{23};$	$21 \equiv -9 \pmod{10}$

- We say "a and b are equivalent to each other in class modulo n"

Concept of congruence



Congruence Relationship

Residue Classes

- A residue class [a] or $[a]_n$ is the set of integers congruent modulo n.

$$
\begin{aligned}
[0] &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} \\
[1] &= \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\} \\
[2] &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} \\
[3] &= \{\ldots, -12, -7, -5, 3, 8, 13, 18, \ldots\} \\
[4] &= \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}
\end{aligned}
$$

Congruent Modulo

- Properties of the congruences
  - If a ≡ b mod n, if n|(a-b) → (a-b) is devisable by n
  - If a ≡ b mod n, implies b ≡ a mod n
  - If a ≡ b mod n and b ≡ c mod n, implies a ≡ c mod n

- Example:
  - 23 ≡ 8 mod 5   → becouse 23-8= 15→ 5|15 = 15=5x3
  - -11 ≡ 5 mod 8 → becouse -11-5= -16→ -16|8 = 16=8x(-2)
  - 81 ≡ 0 mod 27 → becouse 81-0= 81→ 27|81 = 81=27x3

- Examples:
  - 73 ≡ 4 mod 23, then 4 ≡ 73 mod 23, because 4 mod 23 = 73 mod 23
  - 73 ≡ 4 mod 23 and 4 ≡ 96 mod 23, then 73 ≡ 96 mod 23.

- Examples for modular reduction, property 1:
  - Let a= 12 and n= 9 : $12 \equiv 3 \mod 9$
  - Let a= 37 and m= 9: $34 \equiv 7 \mod 9$
  - Let a= -7 and m= 9: $-7 \equiv 2 \mod 9$
- (you should check whether the condition „*n* divides (*a*-*b*)"holds in each of the 3 cases)

Congruent Modulo

- **Self-assessment**
  - State which if any of the following pairs are congruent modulo 7:
    - (a) 10, 3

      $10 \div 7 = 1$ remainder 3, $3 \div 7 = 0$ remainder 3

      so 10 and 3 are congruent modulo 7
    - (b) 12, 5

      $12 \div 7 = 1$ remainder 5, $5 \div 7 = 0$ remainder 5

      so 12 and 5 are congruent modulo 7
    - (c) 14, 6

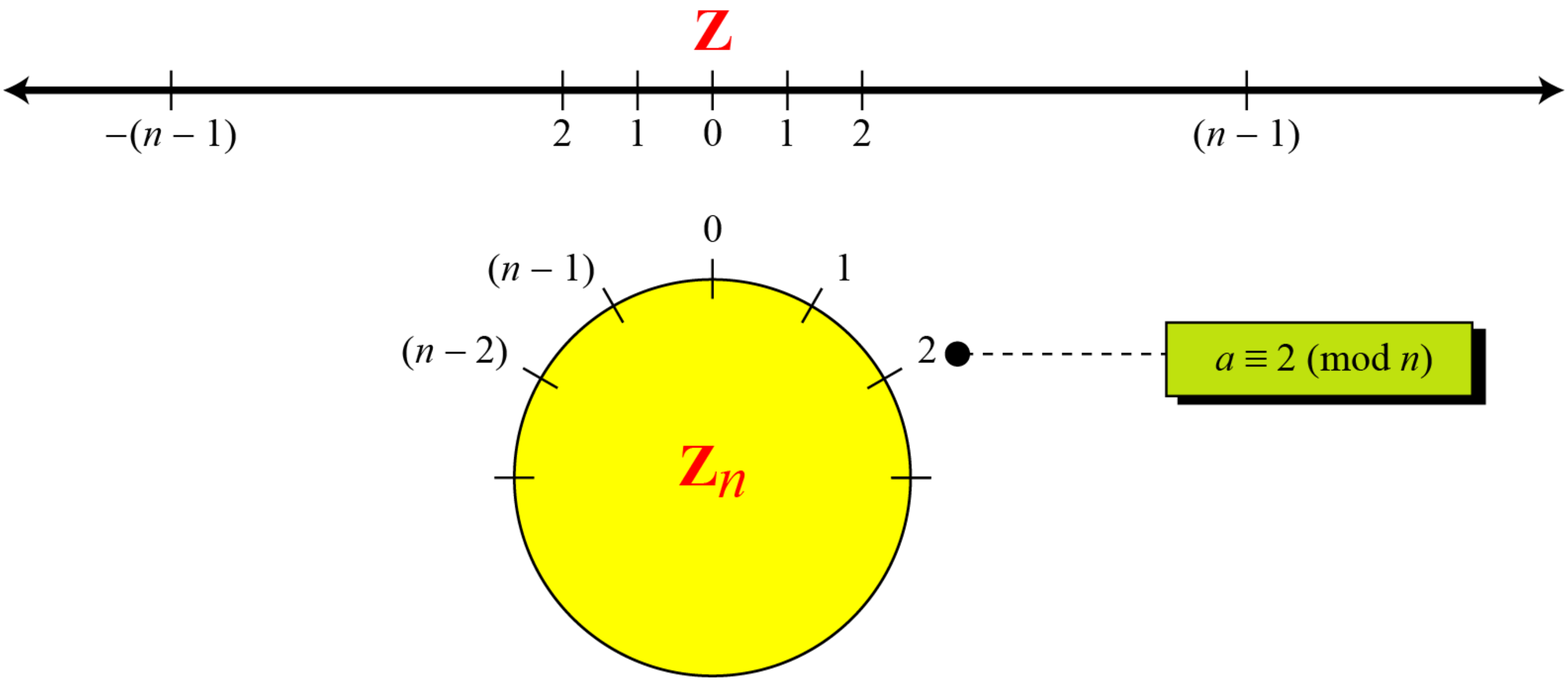
      $14 \div 7 = 2$ remainder 0, $6 \div 7 = 0$ remainder 6

      so 14 and 6 are not congruent modulo 7
    - (d) 26, 12

      $26 \div 7 = 3$ remainder 5, $12 \div 7 = 1$ remainder 5

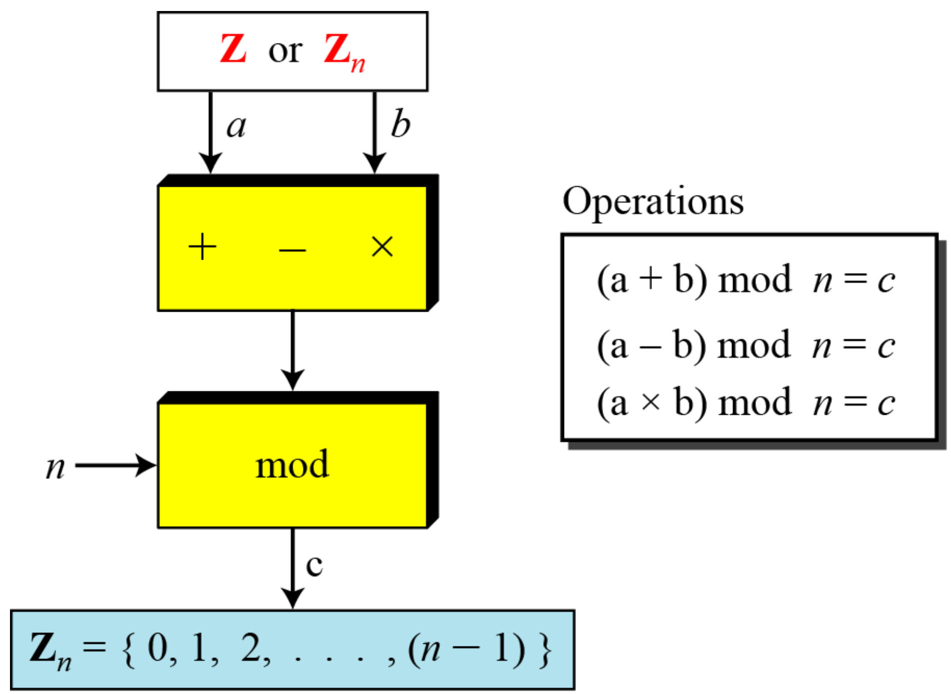
      so 26 and 12 are congruent modulo 7

Comparison of Z and Z_n using graphs



Operation in Z_n

- The three binary operations that we discussed for the set **Z** can also be defined for the set Z_n. The result may need to be mapped to Z_n using the *mod* operator.



Operation in Z_n

Example :

- Perform the following operations (the inputs come from Z_n):
  - a. Add 7 to 14 in Z_{15}.
  - b. Subtract 11 from 7 in Z_{13}.
  - c. Multiply 11 by 7 in Z_{20}.

- Solution

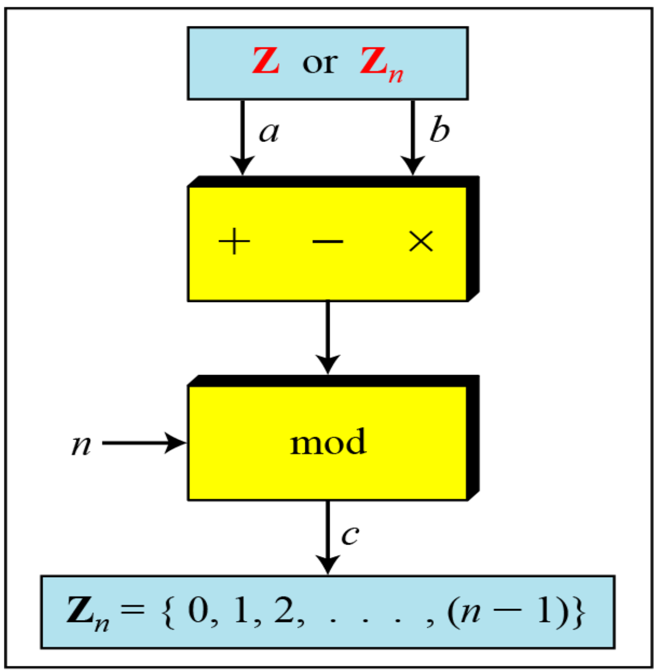
$$(14 + 7) \bmod 15 \quad \rightarrow \quad (21) \bmod 15 = 6$$
$$(7 - 11) \bmod 13 \quad \rightarrow \quad (-4) \bmod 13 = 9$$
$$(7 \times 11) \bmod 20 \quad \rightarrow \quad (77) \bmod 20 = 17$$

Operation in Z_n

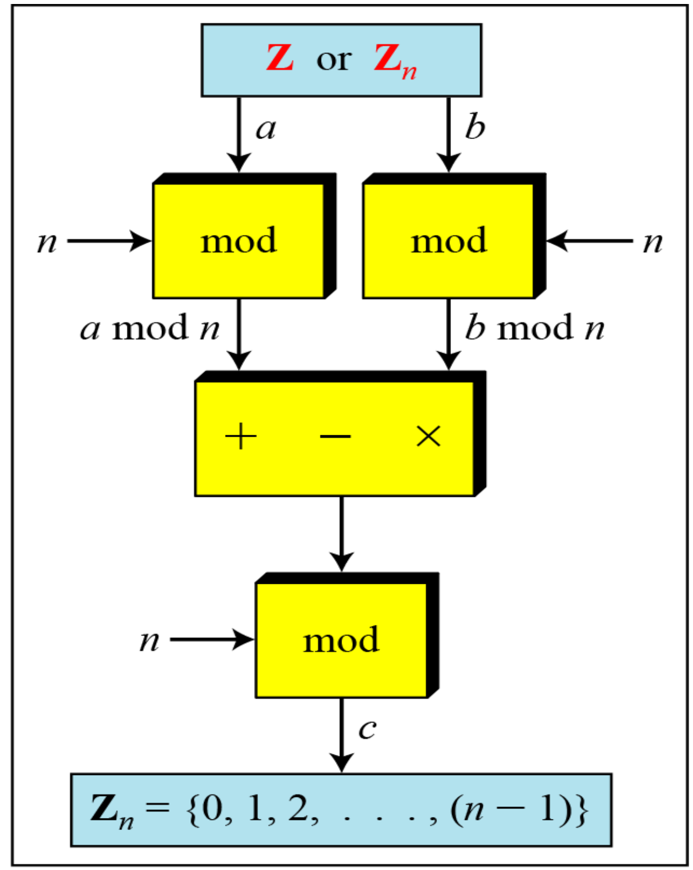
- Properties

First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Properties of mode operator



a. Original process



b. Applying properties

Example:

- The following shows the application of the above properties:

1. $(1{,}723{,}345 + 2{,}124{,}945) \bmod 11 = (8 + 9) \bmod 11 = 6$
2. $(1{,}723{,}345 - 2{,}124{,}945) \bmod 11 = (8 - 9) \bmod 11 = 10$
3. $(1{,}723{,}345 \times 2{,}124{,}945) \bmod 11 = (8 \times 9) \bmod 11 = 6$

Modular Arithmetic

- Properties:
- [(a mod n) + (b mod n)] mod n = (a + b) mod n
- [(a mod n) - (b mod n)] mod n = (a - b) mod n
- [(a mod n) * (b mod n)] mod n = (a * b) mod n
- Compute: (54 + 49) mod 15
  - (54 + 49) mod 15 = 103 mod 15 = 13
  - 54 mod 15 = 9
  - 49 mod 15 = 4
  - (54 mod 15 + 49 mod 15) = 9 + 4 = 13
  - (54 mod 15 + 49 mod 15) mod 15 = 13 mod 15 = 13
- Compute (42 + 52) mod 15
  - (42 + 52) mod 15 = 94 mod 15 = 4
  - 42 mod 15 = 12
  - 52 mod 15 = 7
  - (42 mod 15 + 52 mod 15) = 12 + 7 = 19
  - (42 mod 15 + 52 mod 15) mod 15 = 19 mod 15 = 4

Modular Arithmetic

- Propperties (a * b) mod n = (a mod n * b mod n) mod n
- Compute: (54 * 49) mod 15
  - (54 * 49) mod 15 = 2646 mod 15 = 6
  - 54 mod 15 = 9
  - 49 mod 15 = 4
  - (54 mod 15 * 49 mod 15) = 9 * 4 = 36
  - (54 mod 15 * 49 mod 15) mod 15 = 36 mod 15 = 6
- Compute (42 * 52) mod 15
  - (42 * 52) mod 15 = 2184 mod 15 = 9
  - 42 mod 15 = 12
  - 52 mod 15 = 7
  - (42 mod 15 * 52 mod 15) = 12 * 7 = 84
  - (42 mod 15 * 52 mod 15) mod 15 = 84 mod 15 = 9

Modular Arithmetic

- Properties:
- (a * b * c) mod n = ((a mod n) * (b mod n) * (c mod n)) mod n
- (a * b * c) mod n = ((((a mod n) * (b mod n)) mod n) * (c mod n)) mod n
- (a * b * c * d) mod n = ((a mod n) * (b mod n) * (c mod n) * (d mod n)) mod n
- Similarly, (a * b * c * d * e) mod n….

Greatest Common Divisor (GCD)

- **Greatest common Divisor:** The Greatest common divisor (GCD) of two or more numbers is **the largest number which will divide into each of them exactly (that is, without leaving any remainder)**. The GCD can be found by calculating the prime factors of each of the numbers, then finding the **product** of those **prime factors** that are common
- **Example1:** Find the GCD of **48** and **252**:
  - **48** $= 2 \times 2 \times \mathbf{2} \times \mathbf{2} \times \mathbf{3}$
  - **252** $= \mathbf{2} \times \mathbf{2} \times \mathbf{3} \times 3 \times 7$
  - The common factors are those I have highlighted. So the gcd is the product of all common prime factors:

    $2 \times 2 \times 3 = 12$. So the **GCD(48, 252)= 12**

Greatest Common Divisor (GCD)

- **Example2:** Find the GCD of **84**and **30**:
  - **84** $= 2 \times \mathbf{2} \times \mathbf{3} \times 7$
  - **30** $= \mathbf{2} \times \mathbf{3} \times 5$
  - The common factors are those I have highlighted: $\mathbf{2} \times \mathbf{3} = \mathbf{6}$. So the **greatest common divisor** is **6**
- **Example3:** Find the GCD of **60**, **84** and **150**:
  - **60** $= 2 \times \mathbf{2} \times \mathbf{3} \times 5$
  - **84** $= 2 \times \mathbf{2} \times \mathbf{3} \times 7$
  - **150** $= \mathbf{2} \times \mathbf{3} \times 5 \times 5$
  - The common factors are those I have highlighted: $\mathbf{2} \times \mathbf{3} = \mathbf{6}$. So the **greatest common divisor** is **6**

Greatest Common Divisor (GCD)

- **self-assessment**
  - **What is the greatest common divisor of:**
    - **(a) 68 and 128**
      - **68** $= \mathbf{2} \times \mathbf{2} \times 17$ **128** $= \mathbf{2} \times \mathbf{2} \times 2 \times 2 \times 2 \times 2 \times 2$
      - The common factors are those that I have highlighted: $\mathbf{2} \times \mathbf{2} = \mathbf{4}$. So the **greatest common divisor** is **4**
    - **(b) 27 and 90**
      - **27** $= 3 \times \mathbf{3} \times \mathbf{3}$ **90** $= 2 \times \mathbf{3} \times \mathbf{3} \times 5$
      - The common factors are those that I have highlighted: $\mathbf{3} \times \mathbf{3} = \mathbf{9}$. So the **greatest common divisor** is **9**
    - **(c) 46 and 72**
      - **46** $= \mathbf{2} \times 23$ **72** $= \mathbf{2} \times 2 \times 2 \times 3 \times 3$
      - I have highlighted the only common factor here, which is **2**. So the **greatest common divisor** is **2**

Euclidean Algorithm

Note

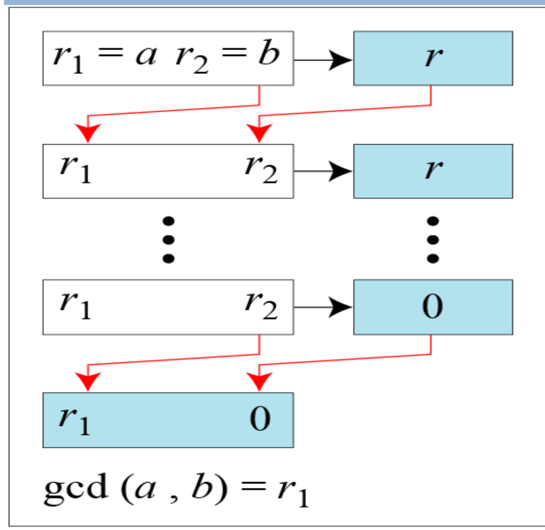
But: Factoring is complicated (and often infeasible) for large numbers. A common problem in number theory

Note **Euclidean Algorithm**

Fact 1: gcd (a, 0) = a

Fact 2: gcd (a, b) = gcd (b, r), where r is the remainder of dividing a by b

Euclidean Algorithm



a. Process

$r_1 \leftarrow a$; $r_2 \leftarrow b$; (Initialization)

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2$;

$r \leftarrow r_1 - q \times r_2$;

$r_1 \leftarrow r_2$; $r_2 \leftarrow r$;

}

gcd $(a, b) \leftarrow r_1$

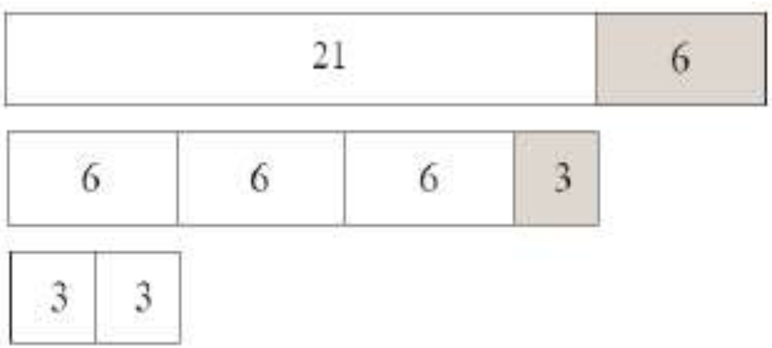
b. Algorithm

Note

When gcd (a, b) = 1, we say that a and b are relatively prime. often want no common factors (except 1) and hence numbers are relatively prime. e.g. GCD(8,15) = 1, hence 8 & 15 are relatively prime

Euclidean Algorithm

- Observation: ***gcd (r0, r1) = gcd (r0 - r1, r1)***
- Core idea:
  - Reduce the problem of finding the gcd of two given numbers to that of the **gcd of two smaller numbers**
  - Repeat process recursively
  - The final ***gcd (ri, 0) = ri*** is the answer to the original problem !
- **Example:** *gcd (r0, r1)* for *r0* = 27 and *r1* = 21



$\gcd(27, 21) = \gcd(1 \cdot 21 + 6, 21) = \gcd(21, 6)$

$\gcd(21, 6) = \gcd(3 \cdot 6 + 3, 6) = \gcd(6, 3)$

$\gcd(6, 3) = \gcd(2 \cdot 3 + 0, 3) = \gcd(3, 0) = 3$

Euclid's GCD Algorithm

- **Euclid's Algorithm** to compute GCD(a,b):
  - `A=a, B=b`
  - `If B = 0 return A = gcd(a, b)`
  - `while B>0`
    - `R = A mod B`
    - `A = B`
    - `B = R`
  - `return A`

$$A_1 = B_1 \times Q_1 + R_1$$

$$A_2 = B_2 \times Q_2 + R_2$$

$$A_3 = B_3 \times Q_3 + R_3$$

$$A_4 = B_4 \times Q_4 + R_4$$

Example GCD(1970,1066)


```
1970 = 1 x 1066 + 904     gcd(1066, 904)
1066 = 1 x 904 + 162      gcd(904, 162)
904 = 5 x 162 + 94        gcd(162, 94)
162 = 1 x 94 + 68         gcd(94, 68)
94 = 1 x 68 + 26          gcd(68, 26)
68 = 2 x 26 + 16          gcd(26, 16)
26 = 1 x 16 + 10          gcd(16, 10)
16 = 1 x 10 + 6           gcd(10, 6)
10 = 1 x 6 + 4            gcd(6, 4)
6 = 1 x 4 + 2             gcd(4, 2)
4 = 2 x 2 + 0             gcd(2, 0)
```

- Compute successive instances of GCD(a,b) = GCD(b,a mod b).
- Note this MUST always terminate since will eventually get a mod b = 0 (ie no remainder left).

Relatively Prime (Coprime)

- Definition
  - Two or more numbers whose **greatest common divisor (factor)** is **1** are said to be **coprime**. (Often the expression **relatively prime** is used as an alternative to coprime but in this course I will stick with the term **relatively prime**)
  - Of course, when the **modulus** itself is a **prime number** then **it will be coprime** with **all the members of the group**, since, by definition, a **prime number has no factors other than 1 and itself**
- For example,
  - 6 and 35 are relatively prime (GCD = 1) while
  - 6 and 8 are not relatively prime (GCD = 2)

FERMAT'S AND EULER'S THEOREMS

- Two theorems that play important roles in public-key cryptography are Fermat's theorem and Euler's theorem.
- **Fermat's Theorem**
- Fermat's theorem states the following: If ***p*** is prime and ***a*** is a positive integer not divisible by ***p, (i.e. a be relatively prime to p)***, then

$$\boxed{a^{p-1} \equiv 1 \bmod p}$$

- Example: a = 7, p = 19

$$
\begin{aligned}
&a = 7, p = 19\\
&7^2 = 49 \equiv 11 \pmod{19}\\
&7^4 \equiv 121 \equiv 7 \pmod{19}\\
&7^8 \equiv 49 \equiv 11 \pmod{19}\\
&7^{16} \equiv 121 \equiv 7 \pmod{19}\\
&a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}
\end{aligned}
$$

FERMAT'S THEOREM

- Second Version
- Alternative form of Fermat's theorem is also useful: If ***p*** is prime and ***a*** is a positive integer then

$$\boxed{a^p \equiv a \bmod p}$$

- This version doesn't require that a be relatively prime to p.

FERMAT'S THEOREM

Example

- Find the result of 6^{10} mod 11.

Solution

- We have 6^{10} mod 11 = 1. This is the first version of Fermat's little theorem where p = 11.

Example

Find the result of 3^{12} mod 11.

Solution

Here the exponent (12) and the modulus (11) are not the same. With substitution this can be solved using

$$3^{12} \bmod 11 = (3^{11} \times 3) \bmod 11 = (3^{11} \bmod 11)\,(3 \bmod 11) = (3 \times 3) \bmod 11 = 9$$

Self-Assessment

$$a^{p-1} \equiv 1 \bmod p$$

- Find 4^{532} mod 11

Solution

Self-Assessment

$$a^{p-1} \equiv 1 \bmod p$$

- Find 4^{532} mod 11

Solution

- $(4)^{532} = (4)^{10*53+2}$
- $(4^{10})^{53}.(4)^2 \ mod\ 11$
- $(1)^{53}.(4)^2 \ mod\ 11$
- $1.(4)^2 \ mod\ 11$
- $16 \ mod\ 11 = 5 \ mod\ 15$

Euler's Totient Function

- For $n \geq 1$, let $\varphi(n)$ denote the number of integer in interval [1, n] which are relatively prime (coprime) to n. the function φ is called the Euller phi of function (or Euller totient function).
- The totient $\varphi(n)$ of a positive integer n greater than 1 is defined to be the number of positive integers less than n that are coprime to n.
- **Euler's totient function** plays a very important role in cryptography.

Euler's Totient Function

- *New problem, important for public-key systems, e.g., RSA:*
- Given the set of the *m* integers {0, 1, 2, …, *n* -1},
- **How many** numbers in the set are **relatively prime to *n*** ?
- Answer: **Euler's Phi function *Φ(n)***
- **Example** for the sets {0,1,2,3,4,5} (*n*=6), and {0,1,2,3,4} (*n*=5)

$$\begin{aligned} \gcd(0,6) &= 6 \\ \gcd(1,6) &= 1 \\ \gcd(2,6) &= 2 \\ \gcd(3,6) &= 3 \\ \gcd(4,6) &= 2 \\ \gcd(5,6) &= 1 \end{aligned}$$

$$\begin{aligned} \gcd(0,5) &= 5 \\ \gcd(1,5) &= 1 \\ \gcd(2,5) &= 1 \\ \gcd(3,5) &= 1 \\ \gcd(4,5) &= 1 \end{aligned}$$

1 and 5 relatively prime to *n* =6, hence ***Φ*(6) = 2** ***Φ*(5) = 4**

Testing one gcd per number in the set is **extremely slow for large *m*.**

Determine $\phi(37)$ and $\phi(35)$.
Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus $\phi(37) = 36$.
To determine $\phi(35)$, we list all of the positive integers less than 35 that are relatively prime to it:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18,
19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

There are 24 numbers on the list, so $\phi(35) = 24$.

Properties of Euller *phi* function:

1. ***Φ(1)= 0.***
2. If p is a prime, then ***Φ(n) = p-1***
3. If n is a product two prime numbers (p,q), not equal (p≠q) and if gcd(p,q)=1, then

   Φ(n) = (p-1)(q-1)

4. If n is a product two prime numbers (p,q), equal (p=q) and if gcd(p,q) ≠ 1, then

   Φ(n) = (p-1)q

5. **If** canonical factorization of *n* known: $\boldsymbol{n = p_1^{e_1} . p_2^{e_2} . \cdots . p_m^{e_m}}$, (where p_i primes and e_i positive integers) then

$$\boldsymbol{\varphi(n) = \prod_{i=1}^{m} \left(p_i^{e_i} - p_i^{e_i - 1}\right)}$$

$$\boxed{\phi(n) = ({p_1}^{e_1} - {p_1}^{e_1 - 1}) \times ({p_2}^{e_2} - {p_2}^{e_2 - 1}) \times \cdots \times ({p_k}^{e_k} - {p_k}^{e_k - 1})}$$

Properties of Euller *phi* function:

Note

The difficulty of finding **φ(n)** depends on the difficulty of finding the factorization of n. Thus, finding **φ(n)** is computationally easy if factorization of n is known (otherwise the calculation of **φ(n)** becomes computationally infeasible for large numbers)

- General formula for Euler's Totient Function

$$\phi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_n}\right)$$

- Where $\boldsymbol{p_1}, \boldsymbol{p_2}, \boldsymbol{p_3}, \ldots, \boldsymbol{p_n}$ are **prime factors** of ***n***

Properties of Euller *phi* function:

- As **an example** of its use, I'll calculate the Euler Totient Function **ø**(m) where ***m*** = 60:
  - 60 = 2 × 2 × 3 × 5
  - So 2, 3 and 5 are the prime factors of 60
  - Using the general formula for Euler's Totient Function:

$$\emptyset(60) = 60 \times \left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{3}\right)\left(1 - \tfrac{1}{5}\right)$$
$$= 60 \times \tfrac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 16$$

- Using the Rule # 5 for Euler's Totient Function:

$$\boxed{\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \cdots \times (p_k^{e_k} - p_k^{e_k-1})}$$

- We can write $60 = 2^2 \times 3^1 \times 5^1$. Then

$$\phi(60) = (2^2 - 2^1) \times (3^1 - 3^0) \times (5^1 - 5^0)$$
$$= (4 - 2) \times (3 - 1) \times (5 - 1) = (2)(2)(4) = 16$$

Properties of Euller *phi* function:

- Example:
  - What is the value of $\phi(13)$?

Solution

  - Because 13 is a prime, $\phi(13) = (13 - 1) = 12$.

- Example:
  - If $p=11$ and $q=7$ and $n= 11\times 7 = 77$
  - What is the value of $\phi(77)$?

Solution

  - Because 77 is a product two prime number, then:

$$\phi(n) = (p - 1)(q - 1)$$

$$\phi(77) = (11 - 1)(7 - 1) = (10)(6) = \mathbf{60}.$$

Properties of Euller *phi* function:

- Example:
  - If p=7 and q=7 and n= 7×7 = 49
  - Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$?
  - What is the value of $\phi(77)$?

Solution

- No. The third rule applies when *p* and *q* are relatively prime and $p \neq q$.
- Here you have two options:
  - According to formula 3, $\phi(49)$ compute as follows:
    - Because 49 is a product two prime number, but equal then:

      $\phi(n) = (p - 1)\, q = \quad \phi(49) = (7 - 1)\, 7 = (6)(7) =$ **42**.
  - According to formula 5, $\phi(49)$ compute as follows
    - $49 = 7^2$. We need to use the fifth rule: $\phi(49) = 7^2 - 7^1 =$ **42**.

- What is the number of elements in $Z_{14}*$?
- Solution
- The answer is $\phi(14) = \phi(7) \times \phi(2) = 6 \times 1 = 6$. The members are 1, 3, 5, 9, 11, and 13.

Note

Interesting point: If $n > 2$, the value of $\phi(n)$ is even.

Euler’s Theorem

- ***First Version :*** States that for every ***a*** and ***n*** that are relatively prime:

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

- ***Second Version :*** the first form of Euler’s theorem [Equation (1)] requires that ***a*** be relatively prime to ***n***, but this form does not.

$$\boxed{a^{k \times \phi(n) + 1} \equiv a \pmod{n}} \quad \ldots\ldots\ldots\ldots(2)$$

- The second version of Euler’s theorem is used in the RSA cryptosystem.

Example

- Find the result of $6^{24} \bmod 35$.

Solution

- We have $6^{24} \bmod 35 = 6^{\phi(35)} \bmod 35 = 1$.

Example

- Find the result of $20^{62} \bmod 77$.

Solution

- If we let $k = 1$ on the second version, we have

$$20^{62} \bmod 77 = (20 \bmod 77)\,(20^{\phi(77)\,+\,1} \bmod 77) \bmod 77$$
$$= (20)(20) \bmod 77 = 15.$$

Self-Assessment

- Find 7^{90} mod 15

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Solution

Self-Assessment

- Find 7^{90} mod 15

Solution

- Find $\varphi(15)=8$
- $(7)^{88}.(7)^2 \equiv 1\, mod\ 15$
- $(7^8)^{11}.(7)^2 \equiv 1\, mod\ 15$
- $(1)^{11}.(7)^2 \equiv 1\, mod\ 15$
- $1.(7)^2 \equiv 1\, mod\ 15$
- $49 \equiv 1\, mod\ 15 \rightarrow 4 \equiv 1\, mod\ 15$

$$a^{\phi(n)} \equiv 1\ (mod\ n)$$

$$GCD\ (7, 15) \stackrel{?}{=} 1$$

$$7^8 \equiv 1\, mod\ 15$$

Inverses

When we are working in modular arithmetic, we often need to find the inverse of a number relative to an operation. We are normally looking for an additive inverse (relative to an addition operation) or a multiplicative inverse (relative to a multiplication operation).

Additive Inverse

- In Z_n, two numbers **a** and **b** are additive inverses of each other if

$$a + b \equiv 0 \pmod{n}$$

In modular arithmetic, each integer has an additive inverse. The sum of an integer and its additive inverse is congruent to 0 modulo n.

Additive Inverse

Example

- Find all additive inverse pairs in Z_{10}.

Solution

- The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

Multiplicative Inverse

- In Z_n, two numbers a and b are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

- In modular arithmetic, an integer may or may not have a multiplicative inverse.
- When it does, the product of the integer and its multiplicative inverse is congruent to 1 modulo n.

Multiplicative Inverse

Example

Find the multiplicative inverse of 8 in Z_{10}.

Solution

There is no multiplicative inverse because gcd (10, 8) = 2 $\neq$ 1. In other words, we cannot find any number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

Multiplicative Inverse

Example

Find all multiplicative inverses in Z_{10}.

Solution

There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse.

Multiplicative Inverse

- The General formula for inverse is:

$$d = e^{-1} \, mod \, \varphi(n)$$

$$e.d \equiv 1 \, mod \, \varphi(n)$$

- There are set of algorithm to find the inverse, like:
  - Exhaustive search algorithm
  - Extended Euclidean algorithm
  - Euller's Theorem

Exhaustive search algorithm

- Choose two prime numbers (P=3, q=7)
- Compute the Modula as $n = p \times q = 3 \times 7 = 21$
- Compute $\varphi(n)$=(p-1)(q-1)→ $\varphi(n)$ (3 -1)(7-1) = 12
- Choose the public key (e) such that:
  - $1 < e < \varphi(n)$
  - GCD(e, $\varphi(n)$)=1
  - e=5
- Compute the invers as follows:
  - $e.d \equiv 1 \; mod \; \varphi(n)$
  - Now try to find d by substituting starting from up to satisfy the above equation.
    - 1→ 5 . 1 mod 12 = 5 ≠ 1 ✗
    - 2→ 5.2 mod 12 = 10 ≠ 1 ✗
    - 3→ 5.3 mod 12 = 3 ≠1 ✗
    - 4→ 5.4 mod 12= 8 ≠ 1 ✗
    - 5→ 5.5 mod 12 =1 ✓
- then d=5

Extended Euclidean Algorithm

- The extended Euclidean algorithm finds the multiplicative inverses of b in **Z_n** when **n** and **b** are given and **gcd (n, b) = 1**.
- The multiplicative inverse of b is the value of t after being mapped to Z_n.

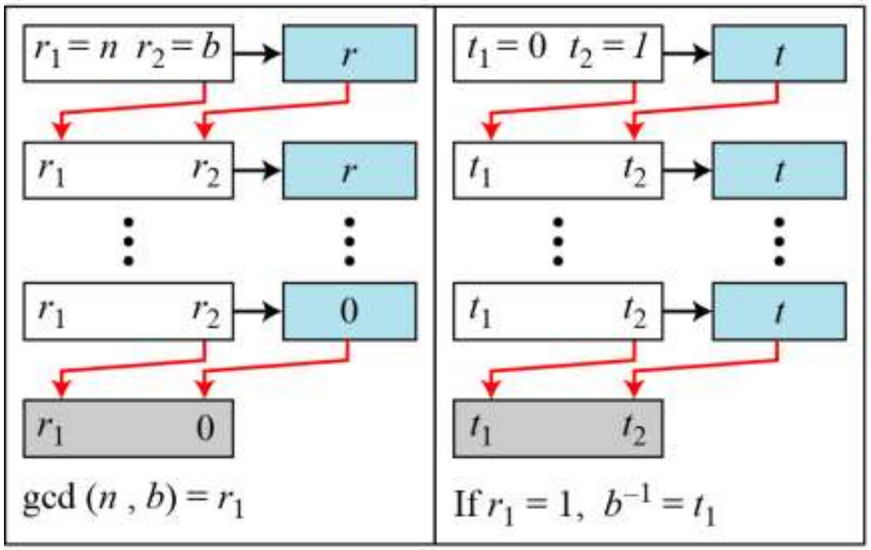
Extended Euclidean Algorithm

- We now proceed to look at an extension to the Euclidean algorithm that will be important for later computations in the area of finite fields and in encryption algorithms, such as RSA.
- For given integers *a* and *b*, the extended Euclidean algorithm not only calculates the greatest common divisor *d* but also two additional integers *s* and *t* that satisfy the following equation.

$$s \times a + t \times b = \gcd(a, b)$$

- The extended Euclidean algorithm can calculate the gcd (a, b) and at the same time calculate the value of s and t.

Extended Euclidean Algorithm



a. Process

$r_1 \leftarrow n; \qquad r_2 \leftarrow b;$

$t_1 \leftarrow 0; \qquad t_2 \leftarrow 1;$

while $(r_2 > 0)$

{

$q \leftarrow r_1 \,/\, r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2; \qquad r_2 \leftarrow r;$

$t \leftarrow t_1 - q \times t_2;$

$t_1 \leftarrow t_2; \qquad t_2 \leftarrow t;$

}

if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

b. Algorithm

if $t_1 < 0$ then $t_1 \leftarrow n + t_1$

Extended Euclidean Algorithm

Example 2.25

- Find the multiplicative inverse of 11 in Z_{26}.
- Solution

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	−2
2	11	4	3	1	−2	5
1	4	3	1	−2	5	−7
3	3	1	0	5	−7	26
	1	0		−7	26	

- The gcd (26, 11) is 1; the inverse of 11 is −7 or 19. if $t_1 < 0$ then $t_1 \leftarrow n + t_1 = 26 + (-7) = 19$

Euler's Theorem to find Inverse

- Multiplicative Inverses
- Euler's theorem can be used to find multiplicative inverses modulo a composite.

$$\boxed{a^{-1} \bmod n = a^{\phi(n)-1} \bmod n}$$

- Example:
- The answers to multiplicative inverses modulo a composite can be found without using the extended Euclidean algorithm if we know the factorization of the

a. $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{59} \bmod 77 = 29 \bmod 77$

b. $7^{-1} \bmod 15 = 7^{\phi(15)-1} \bmod 15 = 7^{7} \bmod 15 = 13 \bmod 15$

c. $60^{-1} \bmod 187 = 60^{\phi(187)-1} \bmod 187 = 60^{159} \bmod 187 = 53 \bmod 187$

d. $71^{-1} \bmod 100 = 71^{\phi(100)-1} \bmod 100 = 71^{39} \bmod 100 = 31 \bmod 100$