

CS 441 Discrete Mathematics for CS Lecture 12

Euclid algorithm. Modular arithmetic.

Milos Hauskrecht

milos@cs.pitt.edu

5329 Sennott Square

Integers and division

- **Number theory** is the branch of mathematics that explores the integers and their properties.
- **Integers:**
 - \mathbf{Z} integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$
 - \mathbf{Z}^+ positive integers $\{1, 2, \dots\}$
- Number theory has many applications within computer science, including:
 - Storage and organization of data
 - Encryption
 - Error correcting codes
 - Random numbers generators

Primes and Composites

Definition: A positive integer p that greater than 1 and that is divisible only by 1 and by itself (p) is called **a prime**.

Examples: 2, 3, 5, 7, ...

$1 \mid 2$ and $2 \mid 2$, $1 \mid 3$ and $3 \mid 3$, etc

Definition: A positive integer that is greater than 1 and is not a prime is called **a composite**.

Examples: 4, 6, 8, 9, ...

Why? $2 \mid 4$, $3 \mid 6$ or $2 \mid 6$, etc

The Fundamental theorem of Arithmetic

Fundamental theorem of Arithmetic:

- Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

- $12 = ?$

The Fundamental theorem of Arithmetic

Fundamental theorem of Arithmetic:

- Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

- $12 = 2*2*3$
- $21 = ?$

The Fundamental theorem of Arithmetic

Fundamental theorem of Arithmetic:

- Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

- $12 = 2*2*3$
- $21 = 3*7$

The Fundamental theorem of Arithmetic

Fundamental theorem of Arithmetic:

- Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

- $12 = 2 \cdot 2 \cdot 3$
- $21 = 3 \cdot 7$
- Process of finding out factors of the product: **factorization**.

Division

Let a be an integer and d a positive integer. Then there are unique integers, q and r , with $0 \leq r < d$, such that

$$a = dq + r.$$

Definitions:

- a is called the **dividend**,
- d is called the **divisor**,
- q is called the **quotient** and
- r the **remainder** of the division.

Relations:

- $q = a \operatorname{div} d$, $r = a \operatorname{mod} d$

Greatest common divisor

Definition: Let a and b are integers, not both 0. Then the largest integer d such that $d \mid a$ and $d \mid b$ is called **the greatest common divisor** of a and b . The greatest common divisor is denoted as $\gcd(a,b)$.

Examples:

- $\gcd(24,36) = ?$
- 12 (start with 2,3,4,6,12)
- $\gcd(11,23) = 1$

Greatest common divisor

A systematic way to find the gcd using factorization:

- Let $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_k^{b_k}$
- $\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} p_3^{\min(a_3,b_3)} \dots p_k^{\min(a_k,b_k)}$

Examples:

- $\gcd(24,36) = ?$
- $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$
- $36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$
- $\gcd(24,36) = 2^2 \cdot 3 = 12$

Least common multiple

Definition: Let a and b be two positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b . The **least common multiple** is denoted as **$\text{lcm}(a,b)$** .

Example:

- What is $\text{lcm}(12,9)$ =?
- 36. Both 12 and 9 cleanly divide 36.

Least common multiple

A systematic way to find the lcm using factorization:

- Let $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_k^{b_k}$
- $\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} p_3^{\max(a_3,b_3)} \dots p_k^{\max(a_k,b_k)}$

Example:

- What is $\text{lcm}(12,9)$ =?
- $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$
- $9 = 3 \cdot 3 = 3^2$
- $\text{lcm}(12,9) = 2^2 \cdot 3^2 = 4 \cdot 9 = \mathbf{36}$

Euclid algorithm

Finding the greatest common divisor requires factorization

- $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$, $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \dots p_k^{b_k}$
- $\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} p_3^{\min(a_3,b_3)} \dots p_k^{\min(a_k,b_k)}$
- Factorization can be cumbersome and time consuming since we need to find all factors of the two integers that can be very large.
- Luckily a more efficient method for computing the gcd exists:
- It is called **the Euclidean algorithm**
 - the method is known from ancient times and named after Greek mathematician Euclid.

Euclid algorithm

Assume two numbers 287 and 91. We want $\gcd(287,91)$.

- First divide the larger number (287) by the smaller one (91)
- We get $287 = 3 \cdot 91 + 14$

Euclid algorithm

Assume two numbers 287 and 91. We want $\gcd(287,91)$.

- First divide the larger number (287) by the smaller one (91)
- We get $287 = 3 \cdot 91 + 14$

(1) Any divisor of 91 and 287 must also be a divisor of 14:

- $287 - 3 \cdot 91 = 14$
- Why? $[ak - cbk] = r \rightarrow (a - cb)k = r \rightarrow (a - cb) = r/k$ (must be an integer and thus k divides r)

Euclid algorithm

Assume two numbers 287 and 91. We want $\gcd(287,91)$.

- First divide the larger number (287) by the smaller one (91)
- We get $287 = 3 \cdot 91 + 14$

(1) Any divisor of 91 and 287 must also be a divisor of 14:

- $287 - 3 \cdot 91 = 14$
- Why? $[ak - cbk] = r \rightarrow (a - cb)k = r \rightarrow (a - cb) = r/k$ (must be an integer and thus k divides r)

(2) Any divisor of 91 and 14 must also be a divisor of 287

- Why? $287 = 3bk + dk \rightarrow 287 = k(3b + d) \rightarrow 287/k = (3b + d) \leftarrow 287/k$ must be an integer

Euclid algorithm

Assume two numbers 287 and 91. We want $\gcd(287,91)$.

- First divide the larger number (287) by the smaller one (91)
- We get $287 = 3 \cdot 91 + 14$

(1) Any divisor of 91 and 287 must also be a divisor of 14:

- $287 - 3 \cdot 91 = 14$
- Why? [$ak - cbk = r \rightarrow (a-cb)k = r \rightarrow (a-cb) = r/k$ (must be an integer and thus k divides r)

(2) Any divisor of 91 and 14 must also be a divisor of 287

- Why? $287 = 3bk + dk \rightarrow 287 = k(3b + d) \rightarrow 287/k = (3b + d) \leftarrow 287/k$ must be an integer
- But then $\gcd(287,91) = \gcd(91,14)$

Euclid algorithm

- We know that $\gcd(287,91) = \gcd(91,14)$
- But the same trick can be applied again:
 - $\gcd(91,14)$
 - $91 = 14 \cdot 6 + 7$
- and therefore
 - $\gcd(91,14) = \gcd(14,7)$
- And one more time:
 - $\gcd(14,7) = 7$
 - trivial
- **The result:** $\gcd(287,91) = \gcd(91,14) = \gcd(14,7) = 7$

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558
- $\text{gcd}(666, 558)$ $666 = 1 \cdot 558 + \dots$

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558
- $\text{gcd}(666, 558)$ $666 = 1 \cdot 558 + 108$
 $= \text{gcd}(558, 108)$ $558 = \dots * 108 + \dots$

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558
- $\gcd(666, 558)$ $666 = 1 \cdot 558 + 108$
 $= \gcd(558, 108)$ $558 = 5 \cdot 108 + 18$
 $= \gcd(108, 18)$ $108 =$

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558
- $\gcd(666, 558)$ $666 = 1 \cdot 558 + 108$
 $= \gcd(558, 108)$ $558 = 5 \cdot 108 + 18$
 $= \gcd(108, 18)$ $108 = 6 \cdot 18 + 0$
 $= \mathbf{18}$

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:
- $\gcd(503, 286)$ $503 =$

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:
- $\gcd(503, 286)$ $503 = 1 \cdot 286 + 217$
 $= \gcd(286, 217)$ $286 =$

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:

- $\gcd(503, 286)$ $503 = 1 \cdot 286 + 217$
 $= \gcd(286, 217)$ $286 = 1 \cdot 217 + 69$
 $= \gcd(217, 69)$ $217 =$

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:

- $\gcd(503, 286)$ $503 = 1 \cdot 286 + 217$
 $= \gcd(286, 217)$ $286 = 1 \cdot 217 + 69$
 $= \gcd(217, 69)$ $217 = 3 \cdot 69 + 10$
 $= \gcd(69, 10)$ $69 =$

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:

- $\gcd(503, 286)$
 $= \gcd(286, 217)$
 $= \gcd(217, 69)$
 $= \gcd(69, 10)$
 $= \gcd(10, 9)$
- $503 = 1 \cdot 286 + 217$
 $286 = 1 \cdot 217 + 69$
 $217 = 3 \cdot 69 + 10$
 $69 = 6 \cdot 10 + 9$
 $10 =$

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:

- $\gcd(503, 286)$
 $= \gcd(286, 217)$
 $= \gcd(217, 69)$
 $= \gcd(69, 10)$
 $= \gcd(10, 9)$
 $= \gcd(9, 1) = 1$
- $503 = 1 \cdot 286 + 217$
 $286 = 1 \cdot 217 + 69$
 $217 = 3 \cdot 69 + 10$
 $69 = 6 \cdot 10 + 9$
 $10 = 1 \cdot 9 + 1$

Modular arithmetic

- In computer science we often care about the remainder of an integer when it is divided by some positive integer.

Problem: Assume that it is a midnight. What is the time on the 24 hour clock after 50 hours?

Answer: ?

M. Hauskrecht

Modular arithmetic

In CS we often care about the remainder of an integer when it is divided by some positive integer.

Problem: Assume that it is a midnight. What is the time on the 24 hour clock after 50 hours?

Answer: the result is 2am

How did we arrive to the result:

- Divide 50 with 24. The remainder is the time on the 24 hour clock.
 - $50 = 2 \cdot 24 + 2$
 - so the result is 2am.

M. Hauskrecht

Congruency

Definition: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a-b$. We use the notation $a \equiv b \pmod{m}$ to denote the congruency. If a and b are not congruent we write $a \not\equiv b \pmod{m}$.

Example:

- Determine if 17 is congruent to 5 modulo 6?

Congruency

Definition: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a-b$. We use the notation $a \equiv b \pmod{m}$ to denote the congruency. If a and b are not congruent we write $a \not\equiv b \pmod{m}$.

Example:

- Determine if 17 is congruent to 5 modulo 6?
- $17 - 5 = 12$,
- 6 divides 12
- so 17 is congruent to 5 modulo 6.

Congruency

Theorem. If a and b are integers and m a positive integer. Then $a \equiv b \pmod{m}$ if and only if $(a \bmod m) = (b \bmod m)$.

Example:

- Determine if 17 is congruent to 5 modulo 6?
- $17 \bmod 6 = \dots$

M. Hauskrecht

Congruency

Theorem. If a and b are integers and m a positive integer. Then $a \equiv b \pmod{m}$ if and only if $(a \bmod m) = (b \bmod m)$.

Example:

- Determine if 17 is congruent to 5 modulo 6?
- $17 \bmod 6 = 5$
- $5 \bmod 6 = \dots$

M. Hauskrecht

Congruency

Theorem. If a and b are integers and m a positive integer. Then $a \equiv b \pmod{m}$ if and only if $(a \bmod m) = (b \bmod m)$.

Example:

- Determine if 17 is congruent to 5 modulo 6?
- $17 \bmod 6 = 5$
- $5 \bmod 6 = 5$
- Thus 17 is congruent to 5 modulo 6.

M. Hauskrecht

Congruencies: properties

Theorem 1. Let m be a positive integer. The integers a and b are congruent modulo m if and only if there exists an integer k such that $a = b + mk$.

Example:

- 8 and 35 mod 9
- $35 = 8 + 3 \cdot 9$

Theorem2. Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then:

$$a+c \equiv b+d \pmod{m} \text{ and } ac \equiv bd \pmod{m}.$$

M. Hauskrecht

Modular arithmetic in CS

Modular arithmetic and congruencies are used in CS:

- **Pseudorandom number generators**
 - Generate a sequence of random numbers from some interval
- **Hash functions**
 - identify how to map information that would need to a large sparse table into a small compact table
- **Cryptology**
 - Prevent other people from reading the transmitted messages

M. Hauskrecht

Pseudorandom number generators

- Any randomness in the program is implemented using random number generators that generate a sequence of random numbers from some interval
 - The chance of picking any number in the interval is uniform
- **Pseudorandom number generators**: use a simple formula to define the sequence:
 - The sequence looks like it was generated randomly
 - The next element in the sequence is a deterministic function of the previous element.
 - Typically based on the modulo operation.

Next: the linear congruential method

M. Hauskrecht

Pseudorandom number generators

Linear congruential method

- We choose 4 numbers:
 - the modulus m ,
 - multiplier a ,
 - increment c , and
 - seed x_0 ,such that $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.
- We generate a sequence of numbers $x_1, x_2, x_3 \dots x_n \dots$ such that $0 \leq x_n < m$ for all n by successively using the congruence:
 - $x_{n+1} = a(x_n + c) \bmod m$

M. Hauskrecht

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = (a x_n + c) \bmod m$

Example:

- Assume : $m=9, a=7, c=4, x_0 = 3$
- $x_1 = 7*3+4 \bmod 9 = 25 \bmod 9 = 7$
- $x_2 = 53 \bmod 9 = 8$
- $x_3 =$

M. Hauskrecht

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = a(x_n + c) \bmod m$

Example:

- Assume : $m=9, a=7, c=4, x_0 = 3$
- $x_1 = 7*3+4 \bmod 9 = 25 \bmod 9 = 7$
- $x_2 = 53 \bmod 9 = 8$
- $x_3 = 60 \bmod 9 = 6$
- $x_4 =$

M. Hauskrecht

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = a(x_n + c) \bmod m$

Example:

- Assume : $m=9, a=7, c=4, x_0 = 3$
- $x_1 = 7*3+4 \bmod 9 = 25 \bmod 9 = 7$
- $x_2 = 53 \bmod 9 = 8$
- $x_3 = 60 \bmod 9 = 6$
- $x_4 = 46 \bmod 9 = 1$
- $x_5 =$

M. Hauskrecht

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = a(x_n + c) \bmod m$

Example:

- Assume : $m=9, a=7, c=4, x_0 = 3$
- $x_1 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7$
- $x_2 = 53 \bmod 9 = 8$
- $x_3 = 60 \bmod 9 = 6$
- $x_4 = 46 \bmod 9 = 1$
- $x_5 = 11 \bmod 9 = 2$
- $x_6 =$

M. Hauskrecht

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = a(x_n + c) \bmod m$

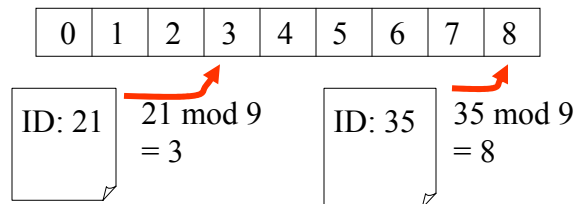
Example:

- Assume : $m=9, a=7, c=4, x_0 = 3$
- $x_1 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7$
- $x_2 = 53 \bmod 9 = 8$
- $x_3 = 60 \bmod 9 = 6$
- $x_4 = 46 \bmod 9 = 1$
- $x_5 = 11 \bmod 9 = 2$
- $x_6 = 18 \bmod 9 = 0$
-

M. Hauskrecht

Hash functions

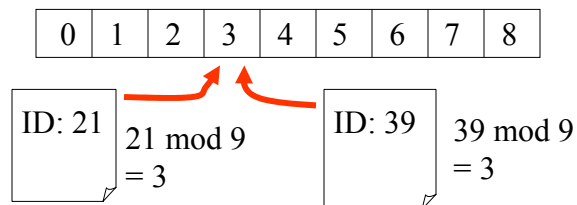
- **Problem:** Given a large collection of records, how can we store and find a record quickly?
- **Solution:** Use a hash function calculate the location of the record based on the record's ID.
- **Example:** A common hash function is
 - $h(k) = k \bmod n$,where n is the number of available storage locations.



M. Hausrecht

Hash functions

- **Problem:** two documents mapped to the same location



M. Hausrecht

Hash functions

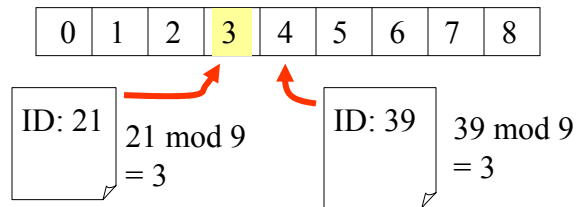
- **Solution 1:** move the next available location
 - Method is represented by a sequence of hash functions to try

$$h_0(k) = k \bmod n$$

$$h_1(k) = (k+1) \bmod n$$

...

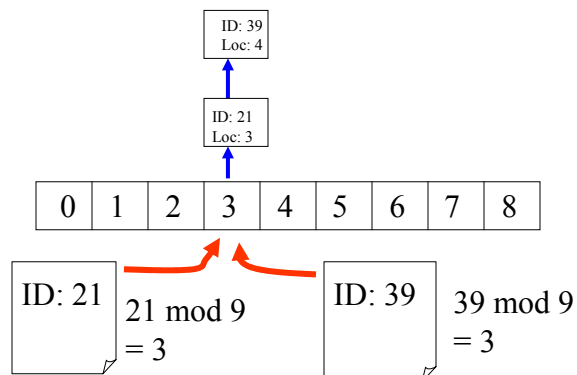
$$h_m(k) = (k+m) \bmod n$$



M. Hausrecht

Hash functions

- **Solution 2:** remember the exact location in a secondary structure that is searched sequentially



M. Hausrecht

Cryptology

Encryption of messages.

- An idea: Shift letters in the message
 - e.g. A is shifted to D (a shift by 3)

How to represent the idea of a shift by 3?

- There are 26 letters in the alphabet. Assign each of them a number from 0,1, 2, 3, .. 25 according to the alphabetical order.

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

M. Hauskrecht

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- **Encrypt message:**

– **I** LIKE DISCRETE MATH

–

M. Hauskrecht

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:

- $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- Encrypt message:

- I LIKE DISCRETE MATH

- L

M. Hausrecht

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:

- $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- Encrypt message:

- I L LIKE DISCRETE MATH

- L O

M. Hausrecht

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Encrypt message:

- I ~~L~~IKE DISCRETE MATH
- L ~~O~~L

M. Hausrecht

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Encrypt message:

- I ~~L~~IKE DISCRETE MATH
- L ~~O~~L

M. Hausrecht

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- **Encrypt message:**
 - I LIKE DISCRETE MATH

 - L OLNH GLYFUHVH PDVK.

M. Hauskrecht

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- **What is method you would use to decode the message:**

M. Hauskrecht

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- What is method would you use to decode the message:
 - $f^{-1}(p) = (p-3) \bmod 26$

M. Hauskrecht

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- What is method would you use to decode the message:
 - $f^{-1}(p) = (p-3) \bmod 26$

– L OLNH GLYFUHVH PDVK

–

M. Hauskrecht

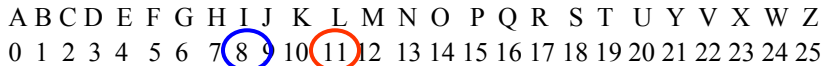
Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25



- What is method would you use to decode the message:
 - $f^{-1}(p) = (p-3) \bmod 26$

- **L** O L N H G L Y F U H V H P D V K

- **I**

M. Hauskrecht

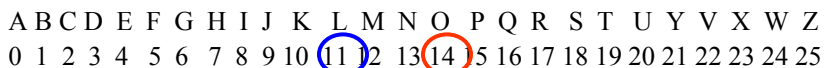
Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25



- What is method would you use to decode the message:
 - $f^{-1}(p) = (p-3) \bmod 26$

- L **O** L N H G L Y F U H V H P D V K

- I **L**

M. Hauskrecht

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
 - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **What is method would you use to decode the message:**
 - $f^{-1}(p) = (p-3) \bmod 26$

– L OLNH GLYFUHVH PDVK

– I LIKE DISCRETE MATH