Congruences

Theorem: Let m be a positive integer.
If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then
$a + c \equiv b + d \pmod m$ and $ac \equiv bd \pmod m$.

Proof:
We know that $a \equiv b \pmod m$ and $c \equiv d \pmod m$ implies that there are integers s and t with
$b = a + sm$ and $d = c + tm$.

Therefore,
$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
$bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.

Hence, $a + c \equiv b + d \pmod m$ and $ac \equiv bd \pmod m$.

The Euclidean Algorithm

The **Euclidean Algorithm** finds the **greatest common divisor** of two integers a and b.

For example, if we want to find gcd(287, 91), we **divide** 287 (the larger number) by 91 (the smaller one):

$287 = 91 \cdot 3 + 14$
$\Rightarrow 287 - 91 \cdot 3 = 14$
$\Rightarrow 287 + 91 \cdot (-3) = 14$

We know that for integers a, b and c,
if a | b, then a | bc for all integers c.

Therefore, any divisor of 91 is also a divisor of $91 \cdot (-3)$.

The Euclidean Algorithm

$287 + 91 \cdot (-3) = 14$

We also know that for integers a, b and c,
if a | b and a | c, then a | (b + c).

Therefore, any divisor of 287 and 91 must also be a divisor of $287 + 91 \cdot (-3)$, which is 14.

Consequently, the greatest common divisor of **287 and 91** must be the same as the greatest common divisor of **14 and 91**:

gcd(287, 91) = gcd(14, 91).

The Euclidean Algorithm

In the next step, we divide 91 by 14:

$91 = 14 \cdot 6 + 7$

This means that gcd(14, 91) = gcd(14, 7).

So we divide 14 by 7:

$14 = 7 \cdot 2 + 0$

We find that 7 | 14, and thus gcd(14, 7) = 7.

Therefore, gcd(287, 91) = 7.

The Euclidean Algorithm

In **pseudocode**, the algorithm can be implemented as follows:

```
procedure gcd(a, b: positive integers)
x := a
y := b
while y ≠ 0
begin
      r := x mod y
      x := y
      y := r
end {x is gcd(a, b)}
```


Representations of Integers

Let b be a positive integer greater than 1.
Then if n is a positive integer, it can be expressed **uniquely** in the form:

$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$,

where k is a nonnegative integer,
$a_0, a_1, \ldots, a_k$ are nonnegative integers less than b,
and $a_k \neq 0$.

Example for b=10:
$859 = 8 \cdot 10^2 + 5 \cdot 10^1 + 9 \cdot 10^0$

Representations of Integers

Example for b=2 (binary expansion):

$(10110)_2 = 1\cdot2^4 + 1\cdot2^2 + 1\cdot2^1 = (22)_{10}$

Example for b=16 (hexadecimal expansion):

(we use letters A to F to indicate numbers 10 to 15)

$(3A0F)_{16} = 3\cdot16^3 + 10\cdot16^2 + 15\cdot16^0 = (14863)_{10}$

Representations of Integers

How can we construct the base b expansion of an integer n?

First, divide n by b to obtain a quotient q_0 and remainder a_0, that is,

$n = bq_0 + a_0$, where $0 \le a_0 < b$.

The remainder a_0 is the rightmost digit in the base b expansion of n.

Next, divide q_0 by b to obtain:

$q_0 = bq_1 + a_1$, where $0 \le a_1 < b$.

a_1 is the second digit from the right in the base b expansion of n. Continue this process until you obtain a quotient equal to zero.

Representations of Integers

Example:
What is the base 8 expansion of $(12345)_{10}$?

First, divide 12345 by 8:
$12345 = 8\cdot1543 + 1$

$1543 = 8\cdot192 + 7$
$192 = 8\cdot24 + 0$
$24 = 8\cdot3 + 0$
$3 = 8\cdot0 + 3$

The result is: $(12345)_{10} = (30071)_8$.

Representations of Integers

procedure base_b_expansion(n, b: positive integers)
q := n
k := 0
while $q \neq 0$
begin
    a_k := q mod b
    $q := \lfloor q/b \rfloor$
    k := k + 1
end
{the base b expansion of n is $(a_{k-1} \ldots a_1a_0)_b$ }

Addition of Integers

How do we (humans) add two integers?

Example:

```
  111      carry
   7583
+ 4932
------
 12515
```

Binary expansions:

```
   1 1      carry
  (1011)2
+ (1010)2
---------
 (10101)2
```


Addition of Integers

Let $a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2$, $b = (b_{n-1}b_{n-2}\ldots b_1b_0)_2$.

How can we **algorithmically** add these two binary numbers?

First, add their rightmost bits:

$a_0 + b_0 = c_0\cdot2 + s_0$,

where s_0 is the **rightmost bit** in the binary expansion of a + b, and c_0 is the **carry**.

Then, add the next pair of bits and the carry:

$a_1 + b_1 + c_0 = c_1\cdot2 + s_1$,

where s_1 is the **next bit** in the binary expansion of a + b, and c_1 is the carry.

Addition of Integers

Continue this process until you obtain c_{n-1}.

The leading bit of the sum is $s_n = c_{n-1}$.

The result is:

$a + b = (s_n s_{n-1} \ldots s_1 s_0)_2$

Addition of Integers

Example:
Add $a = (1110)_2$ and $b = (1011)_2$.

$a_0 + b_0 = 0 + 1 = 0 \cdot 2 + 1$, so that $c_0 = 0$ and $s_0 = 1$.
$a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 \cdot 2 + 0$, so $c_1 = 1$ and $s_1 = 0$.
$a_2 + b_2 + c_1 = 1 + 0 + 1 = 1 \cdot 2 + 0$, so $c_2 = 1$ and $s_2 = 0$.
$a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 \cdot 2 + 1$, so $c_3 = 1$ and $s_3 = 1$.
$s_4 = c_3 = 1$.

Therefore, $s = a + b = (11001)_2$.

Addition of Integers

procedure add(a, b: positive integers)
c := 0
for j := 0 to n-1 {larger integer (a or b) has n digits}
begin
  d := $\lfloor (a_j + b_j + c)/2 \rfloor$
  $s_j := a_j + b_j + c - 2d$
  c := d
end
s_n := c
{the binary expansion of the sum is $(s_n s_{n-1} \ldots s_1 s_0)_2$}

Matrices

A **matrix** is a rectangular array of numbers.
A matrix with m rows and n columns is called an **m×n matrix.**

Example: $A = \begin{bmatrix} -1 & 1 \\ 2.5 & -0.3 \\ 8 & 0 \end{bmatrix}$ is a 3×2 matrix.

A matrix with the same number of rows and columns is called **square**.

Two matrices are **equal** if they have the same number of rows and columns and the corresponding entries in every position are equal.

Matrices

A general description of an m×n matrix $A = [a_{ij}]$:

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix} \qquad \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$$

j-th column of A

$$\begin{bmatrix} a_{i1}, & a_{i2}, & \ldots, & a_{in} \end{bmatrix}$$

i-th row of A

Matrix Addition

Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be m×n matrices.
The sum of A and B, denoted by A+B, is the m×n matrix that has $a_{ij} + b_{ij}$ as its (i, j)th element.
In other words, $A+B = [a_{ij} + b_{ij}]$.

Example:

$$\begin{bmatrix} -2 & 1 \\ 4 & 8 \\ -3 & 0 \end{bmatrix} + \begin{bmatrix} 5 & 9 \\ -3 & 6 \\ -4 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 10 \\ 1 & 14 \\ -7 & 1 \end{bmatrix}$$

Matrix Multiplication

Let A be an m×k matrix and B be a k×n matrix. The **product** of A and B, denoted by AB, is the m×n matrix with (i, j)th entry equal to the sum of the products of the corresponding elements from the i-th row of A and the j-th column of B.

In other words, if AB = $[c_{ij}]$, then

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{ik}b_{kj} = \sum_{t=1}^{k} a_{it}b_{tj}$$

Matrix Multiplication

A more intuitive description of calculating C = AB:

$$A = \begin{bmatrix} 3 & 0 & 1 \\ -2 & -1 & 4 \\ 0 & 0 & 5 \\ -1 & 1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 2 & 1 \\ 0 & -1 \\ 3 & 4 \end{bmatrix}$$

- Take the first column of B
- Turn it counterclockwise by 90° and superimpose it on the first row of A
- Multiply corresponding entries in A and B and add the products: 3·2 + 0·0 + 1·3 = 9
- Enter the result in the upper-left corner of C

Matrix Multiplication

- Now superimpose the first column of B on the second, third, …, m-th row of A to obtain the entries in the first column of C (same order).
- Then repeat this procedure with the second, third, …, n-th column of B, to obtain to obtain the remaining columns in C (same order).
- After completing this algorithm, the new matrix C contains the product AB.

Matrix Multiplication

Let us calculate the complete matrix C:

$$A = \begin{bmatrix} 3 & 0 & 1 \\ -2 & -1 & 4 \\ 0 & 0 & 5 \\ -1 & 1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 2 & 1 \\ 0 & -1 \\ 3 & 4 \end{bmatrix}$$

$$C = \begin{bmatrix} 9 & 7 \\ 8 & 15 \\ 15 & 20 \\ -2 & -2 \end{bmatrix}$$