The Euclidean Algorithm

In pseudocode, the algorithm can be implemented as follows:

```plaintext
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 \textit{uniquely} in the form:

\[
n = a_kb^k + a_{k-1}b^{k-1} + \ldots + a_1b + a_0,
\]

where \( k \) is a nonnegative integer, \( a_k, a_{k-1}, \ldots, a_0 \) 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

Let \( b \) be a positive integer greater than 1. Then if \( n \) is a positive integer, it can be expressed \textit{uniquely} in the form:

\[
n = a_kb^k + a_{k-1}b^{k-1} + \ldots + a_1b + a_0,
\]

where \( k \) is a nonnegative integer, \( a_k, a_{k-1}, \ldots, a_0 \) 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

Let \( b \) be a positive integer greater than 1. Then if \( n \) is a positive integer, it can be expressed \textit{uniquely} in the form:

\[
n = a_kb^k + a_{k-1}b^{k-1} + \ldots + a_1b + a_0,
\]

where \( k \) is a nonnegative integer, \( a_k, a_{k-1}, \ldots, a_0 \) 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

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,

\[
n = bq_0 + a_0, \text{ where } 0 \leq a_0 < b.
\]

The remainder \( a_0 \) is the rightmost digit in the base \( b \) expansion of \( n \). Next, divide \( q_0 \) by \( b \) to obtain:

\[
q_0 = bq_1 + a_1, \text{ where } 0 \leq a_1 < b.
\]

\( a_1 \) 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.

**Example:**

What is the base 8 expansion of \((12345)_{10}\) ?

First, divide 12345 by 8:

\[
12345 = 8 \cdot 1543 + 1
\]

\[
1543 = 8 \cdot 192 + 7
\]

\[
192 = 8 \cdot 24 + 0
\]

\[
24 = 8 \cdot 3 + 0
\]

\[
3 = 8 \cdot 0 + 3
\]

The result is: \((12345)_{10} = (30071)_8\).
Addition of Integers

How do we (humans) add two integers?

Example:

\[
\begin{array}{c}
7583 \\
+ 4932 \\
\hline
12515
\end{array}
\]

Addition of Integers

How do we (humans) add two integers?

Example:

\[
\begin{array}{c}
111 \\
\text{carry}
\end{array}
\]

Binary expansions:

\[
\begin{array}{c}
(1011)_2 \\
+ (1010)_2 \\
\hline
(10101)_2
\end{array}
\]

Addition of Integers

Let \(a = (a_{n-1} a_{n-2} \ldots a_1 a_0)_2\), \(b = (b_{n-1} b_{n-2} \ldots b_1 b_0)_2\).

How can we algorithmically add these two binary numbers?

First, add their rightmost bits:

\[a_0 + b_0 = c_0 \cdot 2 + s_0,\]

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:

\[a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1,\]

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

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

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

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

The result is:

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

 процедура 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 \(m \times n\) matrix.

Example:

\[
A = \begin{bmatrix}
-1 & 1 \\
2.5 & -0.3 \\
8 & 0
\end{bmatrix}
\]

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 $m \times n$ matrix $A = [a_{ij}]$:

\[
A = \begin{bmatrix}
    a_{11} & a_{12} & \cdots & a_{1n} \\
    a_{21} & a_{22} & \cdots & a_{2n} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m1} & a_{m2} & \cdots & a_{mn}
\end{bmatrix}
\]

- $i$-th row of $A$
- $j$-th column of $A$

Matrix Addition
Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be $m \times n$ matrices.
The sum of $A$ and $B$, denoted by $A + B$, is the $m \times n$ 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 $m \times k$ matrix and $B$ be a $k \times n$ matrix.
The product of $A$ and $B$, denoted by $AB$, is the $m \times n$ 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
\[
c_{ij} = a_{ik}b_{kj} + a_{jl}b_{lj} + \ldots + a_{im}b_{mj} = \sum_{k=1}^{k} a_{ik}b_{kj}
\]

Example:
\[
\begin{bmatrix}
    3 & 0 & 1 \\
    -2 & -1 & 4 \\
    0 & 0 & 5 \\
    -1 & 1 & 0
\end{bmatrix}
\times 
\begin{bmatrix}
    2 & 1 \\
    0 & -1 \\
    3 & 4
\end{bmatrix}
= 
\begin{bmatrix}
    9 & 7 \\
    8 & 15 \\
    15 & 20 \\
    -2 & -2
\end{bmatrix}
\]